8e6 Technologies

8e6® Enterprise Reporter

EVALUATION GUIDE

Models: ER HL/SL

Software Version: 5.0.00

Document Version: 01.07.09

Downloaded from www.Manualslib.com manuals search engine

ENTERPRISE REPORTER EVALUATION GUIDE

© 2009 8e6 Technologies

All rights reserved. Printed in the United States of America

Local: 714.282.6111 • Domestic U.S.: 1.888.786.7999 • International: +1.714.282.6111

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior written consent from 8e6 Technologies.

Every effort has been made to ensure the accuracy of this document. However, 8e6 Technologies makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. 8e6 Technologies shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. Due to future enhancements and modifications of this product, the information described in this documentation is subject to change without notice.

Trademarks

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Downloaded from www.Manualslib.com manuals search engine

CONTENTS

8E6 ENTERPRISE REPORTER EVALUATION GUIDE 1

Overview. 1

Note to Evaluators. 1

INSTALL THE ENTERPRISE REPORTER 2

CONFIGURE, TEST THE ENTERPRISE REPORTER 3

Understand the most common and useful features. 3

Use custom Category Groups to narrow your search. 4
- How to create custom Category Groups 4
  - Group Information frame 4
    - How to add a Category Group 4
  - Group Definitions frame 5
    - How to add Categories to a Category Group 5

Use custom User Groups to narrow your search. 6
- How to create User Groups 6
  - Group Information frame 6
    - Add a User Group 6
  - Group Definitions frame 7
    - Define a User Group 7
  - Rebuild Groups 8

Use Enterprise Reporter to conduct an investigation. 9

Use Enterprise Reporter Canned Reports. 10
- How to generate a Canned Report 11
- How to export a Canned Report 13

Use Enterprise Reporter Drill Down Reports. 13
- How to generate a Summary Drill Down Report 14
- Summary Drill Down Report navigation 15
  - Report columns 15
    - Filter columns and buttons 15
    - Count columns 16
    - Sort records by another column 17
  - Navigation tips 17
    - Back button 17
    - Record navigation field 17
- Detail Drill Down Report navigation 18
  - Report type columns 18
  - Page links 19
- Evaluation steps 20
  - Step 1: Select a specific user by Category 20
  - Step 2: Sort by “Filter Action” column 20
  - Step 3: Full URL review 20
  - Step 4: Sort by “Content Type” 21
  - Step 5: Sort by “Search String” 21

Downloaded from www.Manualslib.com manuals search engine

Create a Custom Report for a specific user. 22
How to use the Custom Report Wizard 22
Generate a new Custom Report 22
Next steps for documenting, monitoring specific user activity 24
Export a Custom Report 24
Save a Detail Custom Report 25
Schedule a report to run 27

Appendix A: Samples of Commonly Used Reports. 29
How to generate a Sample Custom Report 29
Report format 30
Examples of available Sample Custom Reports 30
Sample Report 1: “Top 20 Users by Category/User” 30
Sample Report 2: “Top 20 Sites by User/Site” 31
Sample Report 3: “By Category/User/Site” 32

Appendix B: Export and Save Summary Reports. 33
Record exportation tip 33
Step 1: Select records to be exported 33
Step 2: Use header buttons for report customization 33
Step 3: Export a Summary Drill Down Report 34
How to save a Summary Drill Down Report 35
Other Summary Report tools 37
Set Result Limit 37
Report fields 37
Type field 37
Date Scope and Date fields 37
Display and # Records fields 38
Search and Filter String fields 39
Sort by and Order fields 39
Break type field 39
Format field 39
For double-break reports only 40
Amount shown field 40
Records field 40
For pie and bar charts only 40
Generate using field 40
Methods for exporting a Drill Down Report 41
Email option 41
View and print options 42
View and print tools 43
Sample report file formats 43
PDF 44

Downloaded from www.Manualslib.com manuals search engine

8E6 ENTERPRISE REPORTER EVALUATION GUIDE

Overview

Thank you for choosing to review 8e6 Technologies' Enterprise Reporter. The Enterprise Reporter helps administrators manage internal Web-based threats by documenting historical Internet usage information by user.

The Enterprise Reporter is unique in that it is the only dedicated appliance that processes and displays Internet filtering logs without compromising filtering performance or impacting network functions. Built on a dedicated MySQL server database that works in conjunction with 8e6's R3000 Internet filtering appliance, the Enterprise Reporter handles substantial amounts of Internet traffic because of its unique processing approach, which pre-processes and indexes data in a format conducive to high-speed retrieval.

Note to Evaluators

Thank you for taking the time to review 8e6's Enterprise Reporter Appliance. Your interest in our company and product is greatly appreciated.

This Evaluation Guide Is designed to provide product evaluators an efficient way to install, configure and exercise the main product features of the Enterprise Reporter.

Downloaded from www.Manualslib.com manuals search engine

INSTALL THE ENTERPRISE REPORTER

To install the appliance, configure the box and to test reporting is operational please refer to the step-by-step instructions found in the **Enterprise Reporter Quick Start Guide** provided in the box.

Please note that prior to reviewing the Enterprise Reporter you should install the R3000 Internet Filter, which is required for sending logs to the Reporter. See the **R3000 Internet Filter Evaluation Guide** for instructions on how to setup the filter.

***Disable Pop-up Blocking Software**: Please note that a user with pop-up blocking software installed on his/her workstation will need to disable pop-up blocking in order to use the Client.*

***Evaluation Best Practice**: Once the appliance is installed, allow the Enterprise Reporter to run for several days prior to evaluating reports in order to optimize the evaluation experience. This will allow the Enterprise Reporter to accumulate multiple days of data and present more meaningful reports. Having performed these preliminary steps, the Reporter will function properly on day one of the install with some reports showing no data (e.g. canned reports).*

Downloaded from www.Manualslib.com manuals search engine

CONFIGURE, TEST THE ENTERPRISE REPORTER

Understand the most common and useful features

One of the advantages of a hardware appliance, in addition to its compatibility and extremely low profile on the network, is its ease of use. Configuration of the Enterprise Reporter can seem disarmingly simple at times, but when the hardware and software are designed to work together, the levels of complication decrease and robust power and efficiency significantly increase.

The Enterprise Reporter version 5.0 series has an enhanced Web-based user interface that is designed to be very intuitive, utilizing an easy-to-navigate menu tree that is organized to follow the natural flow of an investigation of anomalous Internet activity.

This section of the evaluation guide leads the evaluator, in a linear fashion, through the most common and useful features of the Enterprise Reporter, starting with the elements that should be configured first, then moving on to the usage of the many different types of reports available in the Reporter. You are directed through the normal path of initial setup, and then led through a standard use case that explains how to investigate a violation of your Internet Acceptable Use Policy.

After stepping through this evaluation guide, you will understand how to set up powerful reports that can be e-mailed on a regular basis, thus minimizing the effort required for ongoing configuration of the product. In short, this evaluation guide demonstrates that the Enterprise Reporter is both easy-to-use while at the same time best-in-class in the level of detailed reporting it provides.

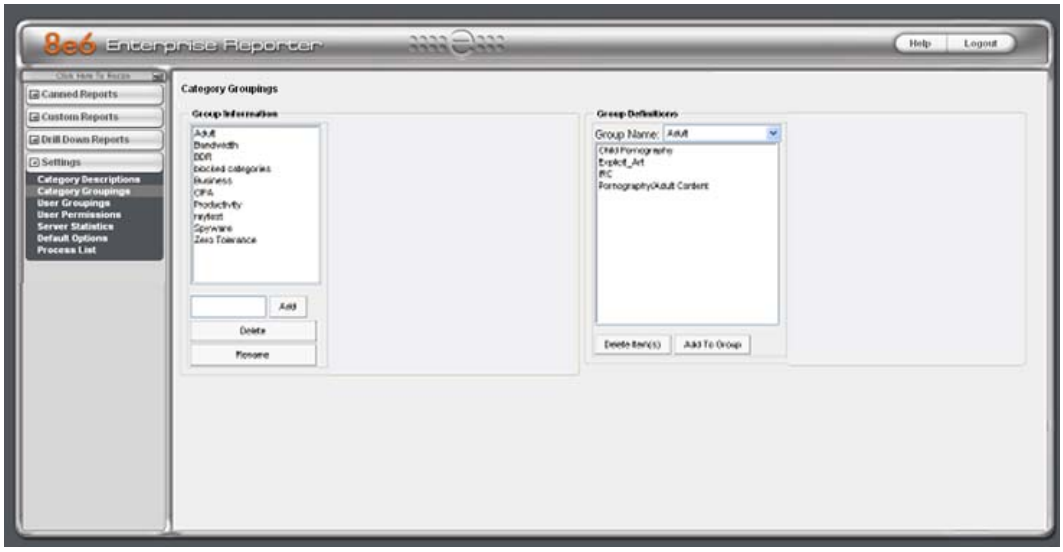
Downloaded from www.Manualslib.com manuals search engine

Use custom Category Groups to narrow your search

Prior to running any reports, there are a few recommended configuration steps that create a more customized experience for the evaluator. The first step is to create category groups, which are customized groupings from the 8e6 library of more than 99 filter categories. For example, most customers prefer to set up a category group for those categories that are not allowed under their organization's Acceptable Use Policy. Creating such a category group reduces the time it takes to identify violations of this policy.

How to create custom Category Groups

To create, edit, or delete a category group, click **Category Groupings** in the Settings menu to display the Category Groupings window in the right panel:



Category Groupings window

The Category Groupings window is comprised of two frames used for setting up and maintaining category groupings: Group Information, and Group Definitions.

Group Information frame

The Group Information frame displays to the left in the Category Groupings window. In this frame you can add, rename, or delete a category group.

Any category groups that were created display in alphanumerical order in the list box in this frame.

How to add a Category Group

1. In the field to the left of the Add button, type in the name for the category group. (For this evaluation, name the category group "Unacceptable Sites".)
2. Click the **Add** button to add this entry to the list box above.

***NOTE**: The category group you added also displays in the Group Name pull-down menu in the Group Definitions frame to the right.*

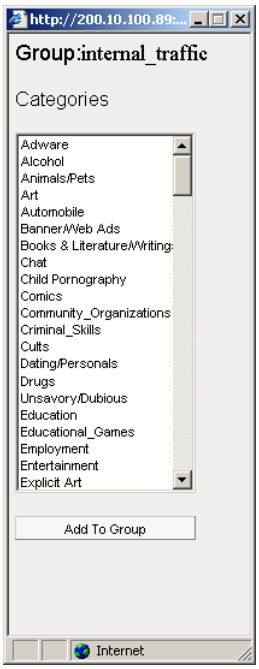
Downloaded from www.Manualslib.com manuals search engine

Group Definitions frame

The Group Definitions frame displays to the right in the Category Groupings window. In this frame you define a category group by specifying which categories will belong to that group.

How to add Categories to a Category Group

1. Select a category group from the Group Name pull-down menu. Any categories previously entered display in the list box in this frame. (For evaluation purposes select “Pornography/Adult Content” as the only category in this category group.)
2. Click the Add To Group button to open the Add To Group pop-up box:



Add To Group

3. Select a category from the pop-up box by clicking on your choice to highlight it.

***TIP**: To select multiple categories, press the Ctrl key on your keyboard and then click on categories to highlight them.*

4. Click the **Add To Group** button in the pop-up box to specify the selected categories to be added to the Group Definitions frame list box.
5. Click the "X" in the upper right corner of the Add To Group pop-up box to close it, and to add all selected categories to the list box in the Group Definitions frame.

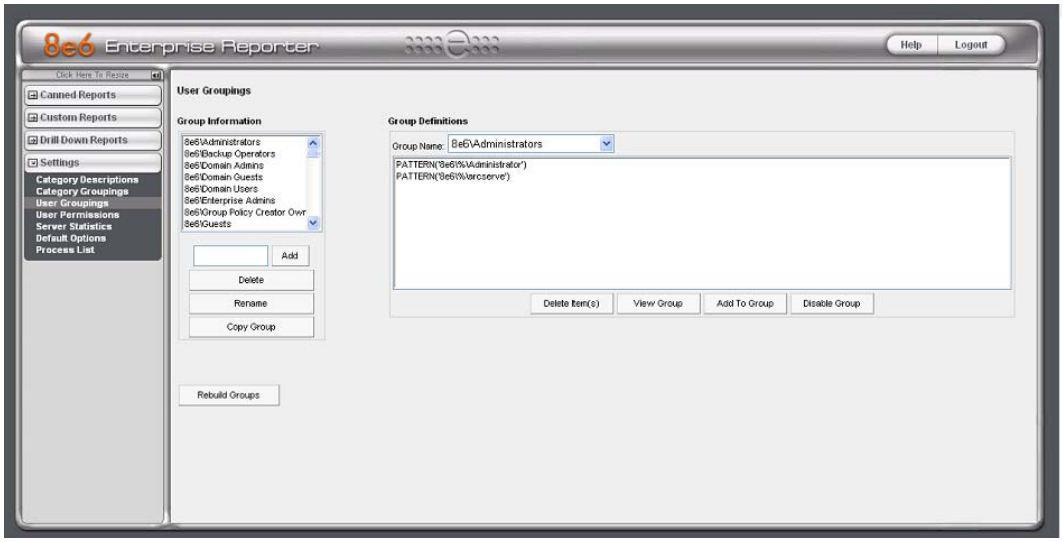
Downloaded from www.Manualslib.com manuals search engine

Use custom User Groups to narrow your search

The next step is to create user groups, which are customized groupings of users that reside on the organization's network. For example, most enterprise customers prefer to set up user groups for each department within the company, and education customers prefer to setup separate user groups for each classroom or grade level. Creating these user groups reduces the time it takes to identify the source of violations of your organization's Acceptable Use Policy.

How to create User Groups

To create, edit, or delete a user group, click **User Groupings** in the Settings menu to display the User Groupings window in the right panel:



User Groupings window

The User Groupings window is comprised of two frames used for setting up and maintaining user groupings: Group Information, and Group Definitions.

Group Information frame

The Group Information frame displays to the left in the User Groupings window. In this frame you can add, rename, or delete a user group.

Any user groups that were created display in the list box in this frame.

Add a User Group

1. In the field to the left of the Add button, type in the name for the user group. (Use "Sales" for this evaluation.)
2. Click the **Add** button to add this entry to the list box above.

***NOTE**: The user group you added also displays in the Group Name pull-down menu in the Group Definitions frame to the right.*

Downloaded from www.Manualslib.com manuals search engine

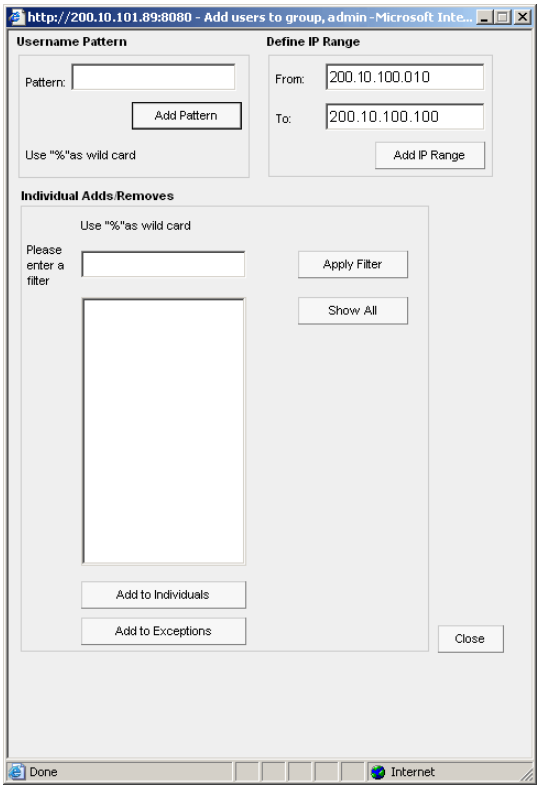
Group Definitions frame

The Group Definitions frame displays to the right in the User Groupings window. In this frame you can view members of a user group, and can define a user group by specifying which users will belong to that group.

Define a User Group

When defining a user group, you can add and/or exclude users to/from that group. Modifications to a user group can be made at any time, as necessary.

1. Select a user group from the **Group Name** pull-down menu. Any users previously entered display in the list box in this frame. (Select “Sales” for this evaluation.)
2. Click the **Add To Group** button to open the pop-up box where you define users to be added/excluded to/from the group:



Add Users to group

***TIPS**: To view a list of all users, go to the Individual Adds/Removes frame and click the Show All button to display the list of users in the list box. To clear your entries in this pop-up box without accepting them, do not click any of the buttons in the frames described below. Instead, click the Close button in the pop-up box, and return to step 1.*

3. Make entries in one of the three frames:
   - **Username Pattern** - This frame is used for including users from a specific group (such as “sales”) on the network. In the **Pattern** field, enter the appropriate characters and wild card “%” to add specified users to the group. For example, type in **sales%** to add anyone to the group who has a “sales” designation on your network. Click the **Add Pattern** button to add the pattern.

Downloaded from www.Manualslib.com manuals search engine

- **Please Enter IP Range** - This frame is used for including users based on a range of IP addresses. For example, you might have one range of IP addresses for sales, and another for admin. Enter the IP address range in the **From** and **To** fields. Click the **Add IP Range** button to add the IP address range.
- **Individual Adds/Removes** - This frame is used for including and/or excluding specified users. Click the **Show All** button to display a list of all users in the list box. To narrow down the list of users, make an entry in the **Please enter a filter** field using the "%" wild card, and click the **Apply Filter** button to only display the users you specified. To select from users in the list box, click on the user(s) to highlight your choice(s). After making all choices, click **Add to Individuals** to include the selected users to the group, or click **Add to Exceptions** to exclude the users from the group.

***TIP**: In the Individual Adds/Removes frame, if you know which users you would like to add/exclude to/from the group, you can bypass the step for showing all users and making your selections. To use this shortcut, enter the criteria in the Please enter a filter field along with the "%" wild card, and then click the Apply Filter button to display your results in the list box.*

4. After you have made your entries, click **Close** to close the pop-up box.

   The following information displays in the Group Definitions frame list box when a selection for the group is made from the Group Name pull-down menu:

   - If an entry was made in the Username Pattern frame, "PATTERN" and the character(s) you entered display(s).
   - If entries were made in the IP Range frame, "IP RANGE('X.X.X.X' AND 'X.X.X.X')" displays, in which 'X.X.X.X' represents the IP address that was entered in the From or To field.
   - If entries were made in the Individual Adds/Removes frame, "INDIVIDUAL (...)" and/or "EXCEPTION (...)" displays, in which '(...)' represents specific details about the entry.

***NOTE**: A combination of any of items above may display in the Group Definitions frame list box, based on entries you made in any of the frames in the pop-up box.*

Rebuild Groups

After making all additions, modifications, or deletions in the User Groupings window, click **Rebuild Groups**.

Downloaded from www.Manualslib.com manuals search engine

Use Enterprise Reporter to conduct an investigation

Once custom category groups and user groups have been created, administrators can begin running their first reports. In most cases, administrators will employ the Enterprise Reporter as a forensic tool to determine if anomalous Internet behavior exists in their organization. In order to facilitate this process, the Enterprise Reporter menu structure is organized to follow the normal process flow of an investigation.

1. First, the administrator is greeted with a dashboard of high-level reports called "**Canned Reports**." By viewing these canned reports, an administrator can quickly determine if there is any anomalous behavior that needs investigation.

   For example, a high level of spyware site activity might be found under a specific username, or a high rate of traffic identified in the "PornographyAdult Content" category. If something is detected that warrants further investigation, one would then proceed to the "**Drill Down Report**" section.

2. The next stage of the investigation is to select the Drill Down Report menu. The Drill Down Report is a multi-dimensional database that allows the user to drill down to the source of any Internet threat.

   For example, if there is unusually high page count in the "Pornography/Adult Content" category, the administrator can drill down into the Category/User section to determine who is viewing this material. Once a specific end user is identified, the administrator can then delve into the detail page view section to see the exact pages that end user has been visiting.

   This detailed information provides a wealth of information on the exact time the page was visited, the user's IP address, whether the site was blocked by the R3000 filter, how it was blocked (e.g. in URL library, blocked keyword, proxy pattern blocking, etc), and the full-length URL. By viewing this detail, the administrator can obtain an accurate gauge of the user's intent—whether the user repeatedly attempted to go to a forbidden site or whether it was an isolated incident.

3. The last stage of an investigation is to document the long-term activity of a policy violator, since most organizations require more than one or two events to reprimand a user. Once the administrator determines the name of the user and the Web sites visited in the Drill Down Report, the next step is to run a custom report. The administrator can run a specific search of the policy violator for a custom time period by selecting the **Custom Report Wizard** option in the Custom Reports menu. When generating this report, a custom time scope, specific category, and name of a specific end user can be specified.

   As an example, the administrator would probably run a custom report for the policy violator by specifying the category "Pornography/Adult Content" and all activity within that category within the last month. The administrator can then save a PDF version of the report for documentation purposes. This custom report provides the necessary forensic information to support any internal reprimand and to protect the organization in the event the incident goes to court.

To summarize, the aforementioned steps were provided to give the user a most-likely use case for the 8e6 Enterprise Reporter. The next section provides a more in-depth view of how to navigate within each of the main sections of the Enterprise Reporter: Canned Reports, Drill Down Reports, and Custom Reports.

Downloaded from www.Manualslib.com manuals search engine

Use Enterprise Reporter Canned Reports

As previously stated, the first thing the administrator will see when logging into the Enterprise Reporter is a dashboard of graphical reports called “Canned Reports”. By viewing these reports, an administrator has an at-a-glance view of any anomalous behavior that warrants an investigation.

Canned reports contain pre-generated data for a specified period of time (Yesterday, Last Week, Last Month, Week to Yesterday, or Month to Yesterday) for any of the following report topics or entities showing Internet activity:

- **Top 20 Users by Blocked Request** - bar chart report that shows the end users with the most attempts to view blocked content as determined by the filter policy.
- **Top 20 Categories by Page Count** - bar chart report based on the total page count for each filtering category set up in the Category Description list from the Settings menu.
- **Top 20 Users by Page Count** - bar chart report based on each end user’s total page count.
- **Top 20 Users by Malware Hit Count** - bar chart report based on each end user’s total hit count from the following categories in the Security, Internet Productivity, and Internet Communication (Instant Messaging) category groups: BotNet, Malicious Code/Virus, Bad Reputation Domains, Spyware, Adware, and IRC.
- **Top 20 Sites by Page Count** - bar chart report based on the total page count for the most popular sites accessed by end users.
- **Top 20 User Groups by Page Count** - bar chart report based on the total page count for each user group set up in the User Groupings list from the Settings menu.
- **Category Comparison** - pie chart report based on the total page count for each filtering category set up in the Category Description list from the Settings menu.
- **User Group Comparison** - pie chart report based on the total page count for each user group set up in the User Groupings list from the Settings menu.

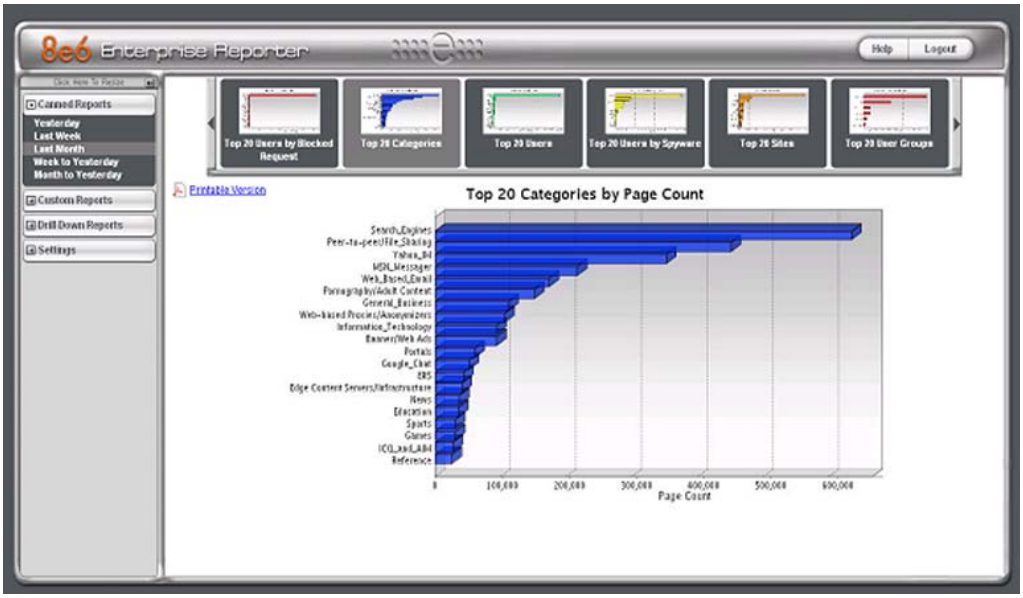
Once you have obtained an overview of Internet activity using canned reports, you can drill down to access more detailed information about specified end user activity.

Downloaded from www.Manualslib.com manuals search engine

How to generate a Canned Report

To generate a canned report:

1. Go to the navigation panel and click **Canned Reports** to display yesterday's Top 20 (Internet Filtering) Categories by Page Count report view in the right panel:



Yesterday's Top 20 Categories by Page Count Report

***TIP**: Click the left arrow or right arrow at the edges of the dashboard to display thumbnail images that are currently hidden.*

***NOTE**: If the ER Server does not contain any data—as on a newly installed unit—the default report page will not show any thumbnail images or bar chart report in the right panel, and the following text displays: "This report cannot be displayed because there is no data to show for this report."*

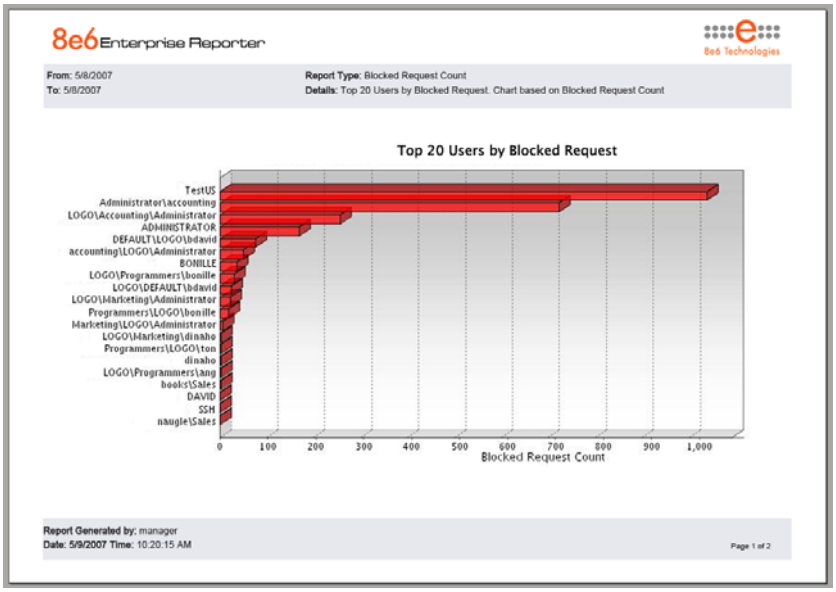
2. Click a menu topic in the navigation panel for the time period to be included in the report: "Yesterday", "Last Week", "Last Month", "Week to Yesterday", or "Month to Yesterday".

3. Click a thumbnail in the dashboard for the selected report option to display as the report view.

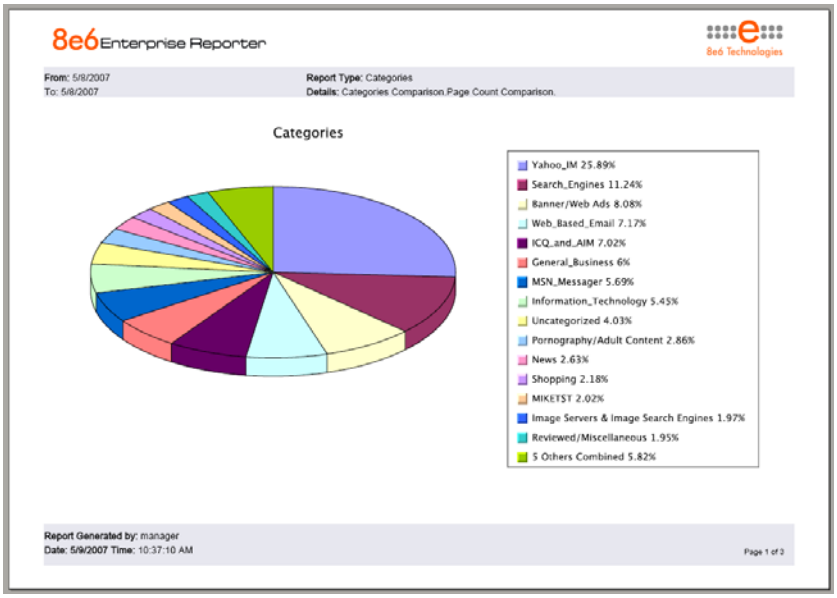
***NOTE**: If necessary, click another time period or thumbnail to display that specified report view in the right panel.*

4. To see details for the generated canned report view, click the Printable Version link to the left, just below the dashboard. This action opens a separate browser window containing the canned report in the PDF format:

Downloaded from www.Manualslib.com manuals search engine



Sample Bar Chart Canned Report



Sample Pie Chart Canned Report

The header of the generated canned report includes the date range, Report Type, and criteria Details.

The body of the first page of the report includes the following information:

- Bar chart - name of category, username, username path, URL or site IP address, or user group name, and corresponding bar graph.
- Pie chart - color-coded pie graph and key showing a maximum of 15 categories or user groups. Any categories or user groups with page counts totaling less than one percent are grouped together under the “Others Combined” label.

The footer of the report includes the username of the person who generated the report (Report Generated by), the Date and Time the report was generated, and Page number.

Downloaded from www.Manualslib.com manuals search engine

The body of the following page(s) of the report includes Count columns and corresponding totals.

The Grand Total and Count display at the end of the report.

***NOTE**: See 'Summary Drill Down Report navigation' for information about report elements referenced above.*

How to export a Canned Report

From the open PDF file, the canned report can be exported in some of the following ways:

- print the report - click the print icon to open the Print dialog box, and proceed with standard print procedures.
- save the report - click the save icon to open the Save a Copy dialog box, and proceed with standard save procedures.

***TIP**: If you saved the report, you can later send it as an email attachment.*

Use Enterprise Reporter Drill Down Reports

In the event that canned reports in the Enterprise Reporter dashboard reveal abnormal activity, the next step in the investigation would be to drill down into the particular category or user information.

This section provides information about "drill down" reports that let you query the database to access more detailed information about end user Internet activity. The following types of reports can be generated:

- **Categories** - includes data in each filter category that was set up for monitoring user activity.
- **IPs** - includes Internet activity by user IP address.
- **Users** - includes Internet activity by username.
- **Sites** - includes activity on Web sites users accessed.
- **Category Groups** - includes activity by category groups, if category groups previously have been set up via the Settings menu.
- **All User Groups** - includes activity by all user groups, if user groups previously have been set up via the Settings menu.
- **Single User Group** - after selecting the user group from a list of available choices, this report shows activity for that user group, if the user group previously has been set up via the Settings menu.

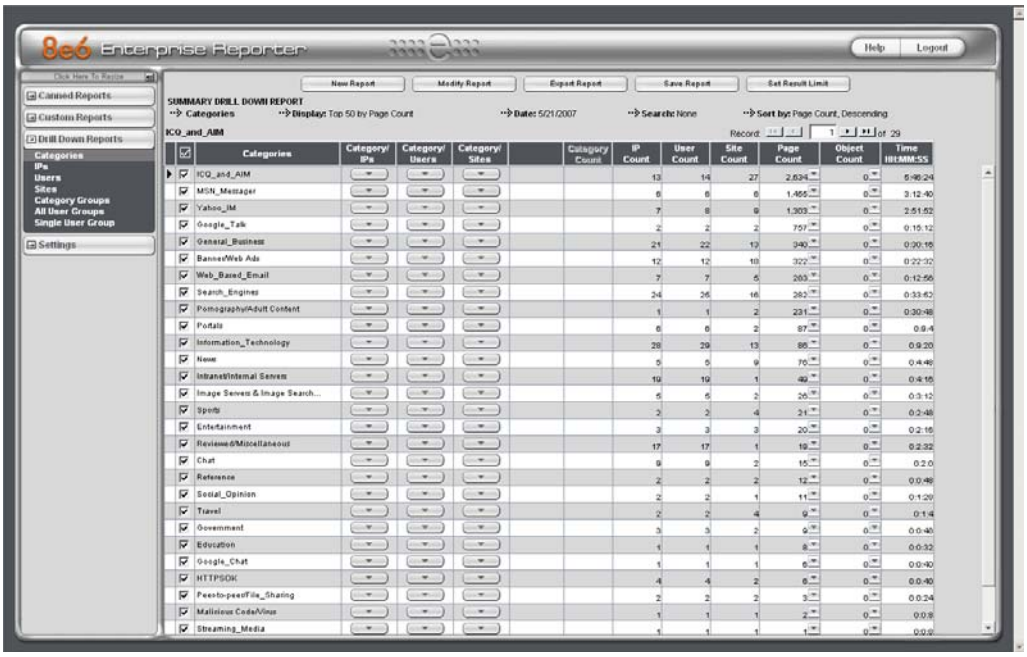
Once you have generated a drill down report view, you can customize your view, save the view, export the view, and/or schedule the report to run at a designated time.

Downloaded from www.Manualslib.com manuals search engine

How to generate a Summary Drill Down Report

To generate a summary drill down report:

1. Go to the navigation panel and click Drill Down Reports to display (by default) today's Categories report view by Page Count in the right panel:



Sample Drill Down Categories Report (Summary report)

2. Click one of the following menu topics in the navigation panel for the type of report you wish to view: Categories, IPs, Users, Sites, Category Groups, All User Groups. (For purposes of this evaluation, select "Categories".)

***NOTE**: As the report is generating, the message: "Please wait for your report to be generated." displays. If no records are available, an alert box opens displaying the message "No records returned!"*

The report view is horizontally organized into three sections:

- Header section - includes buttons for customizing the current view: New Report, Modify Report, Export Report, Save Report, and Set Result Limit. The following information displays beneath the row of buttons: Report type, Display criteria, Date, Search criteria, Sort by criteria. Beneath this row of data, the navigation path for the first record in the current report view displays to the far left. The Record navigation field at far right lets you navigate to a specific record and includes the total number of records.
- Body section - includes rows of records returned by the reporting query. Each row is preceded by a checkbox. For each record, columns of filter buttons display. These buttons are followed by columns of statistics for tracking user activity on the Internet by Category Count, IP Count, User Count, Site Count, Page Count, Object Count, or Time HH:MM:SS. A down arrow displays to the right of the Page Count and Object Count for each record. By clicking the arrow, a detail report view for that record displays.
- Footer section - includes the username of the login ID used for this session (Logged in as).

Downloaded from www.Manualslib.com manuals search engine

3. Use the tools in the right panel to create the desired drill down view.

***NOTE**: See 'Summary Drill Down Report navigation' for information on using the reporting elements described in this sub-section.*

4. The drill down view can be exported, saved, and/or scheduled to run at a specified time.

Summary Drill Down Report navigation

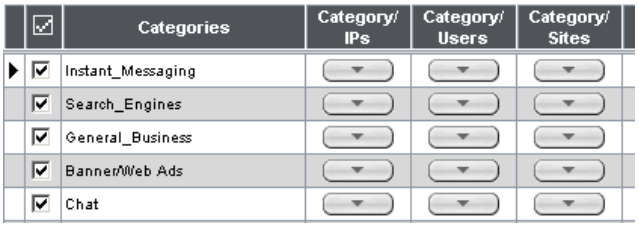
Continuing from the last section, this section is designed to help the administrator learn how to navigate within the Summary Drill Down Report. The Drill Down report is unique in terms of the seemingly endless ways data can be displayed, but it is important to understand all of the functions within this tool in order to generate meaningful reports.

Report columns

Filter and count columns display in the body of drill down report views. These columns are used for specifying additional information to be included for records or for sorting records by a different column.

Filter columns and buttons

Filter columns display after the column containing the record name, and precede the Count columns (Category Count, IP Count, User Count, Site Count, Page Count, Object Count, Time HH:MM:SS). Filter columns include an oblong button for each record in the report view.



Filter columns and buttons

Clicking a specific filter button for a record gives more in-depth analysis on a given record displayed in the current view. For the purposes of this evaluation, try clicking on the oblong button in the "Pornography/Adult Content" row and "Category/Users" column if there is any activity in that category row. This will bring up a view of the top users for this category by page count.

Downloaded from www.Manualslib.com manuals search engine

Count columns

Columns for specified “item counts” display in the body of all drill down report views. The column for the current report type does not display and therefore cannot be selected.

IP Count	User Count	Site Count	Page Count	Object Count	Time HH:MM:SS
63	37	132	35,963	434	95:40:20
95	60	60	6,885	6,088	10:59:0
97	57	116	4,542	6,919	8:19:10
94	56	87	4,458	8,883	8:8:0
30	20	12	3,223	207	7:33:30

Count columns

- **Category Count** - displays the number of categories a user has visited, or the number of categories included within a given site. Categories are set up for the Web access logging device filter via the Settings menu option. It is possible for a site to be listed in more than one category, so even if a user has visited only one site, this column may count the user’s visit in two or three categories.
- **IP Count** - displays the number of sites or categories visited by the IP address on the user’s machine.
- **User Count** - displays the number of individuals who have visited a specific site or category.
- **Site Count** - displays the number of sites a user has visited, or the number of sites in a category. This figure is based on the root name of the site. For example, if a user visits www.espn.com, www.msn.com, and www.foxsports.com, that user will have visited three pages. If that same user additionally visits www.espn.com/scores, the total number of sites visited would still count as three—and not as four—because the latter page is on the original ESPN site that was already counted.
- **Page Count** - displays the total number of pages visited. A user may visit only one site, but visit 20 pages on that site. If a user visits a page with pop-up ads, these items would add to the page count. If a page has banner ads that link to other pages, these items also would factor into the page count. In categories that use a lot of pop-up ads—porn, gambling, and other related sites—the page count usually exceeds the number of objects per page.

  By clicking the arrow to the right of any record in this column, the custom report view displays data for all pages visited, including hyperlinks to those pages (this is covered in greater detail in the next section ‘Detail Drill Down Report navigation’).

***TIP**: If the date range that was specified at the Date Scope field is outside the scope of live data currently stored on the Server, when clicking the arrow button, a warning message displays to inform you that if you wish to proceed, the report will take a longer amount of time to generate.*

- **Object Count** - displays the number of objects on a Web page. All images, graphics, multimedia items, and text items count as objects. The number of objects on a page is generally higher than the number of pages a user visits.

Downloaded from www.Manualslib.com manuals search engine

However, if an advertisement or banner ad (an object on the page) is actually a page from another site, this item would not be classified as an object but as a page, since it comes from a different server. By clicking the arrow to the right of any record in this column, the custom report view displays data for all objects accessed, including hyperlinks to those objects (this is covered in greater detail in the next section 'Detail Drill Down Report navigation').

***NOTE**: Reporting objects is a configurable option in the ER Administrator interface if the customer does not require this degree of detail and/or wants to maximize database storage and reporting performance. See the Enterprise Reporter Administrator User Guide for additional details on this option.*

- **Time HH:MM:SS** - displays the amount of time a user spent at a given site. Each page detected by a user's machine adds to the count. If a browser window is opened to a certain page and left there for an extended time period, and that page is refreshed by either the user or a banner ad, the counter starts again and continues as long as Web activity is detected. If that Web page contains an active banner ad that refreshes the page every 10 to 30 seconds, a user could show an incredibly high page count and many minutes, even though only one page was opened by that user.

Sort records by another column

To sort records in ascending/descending order by a specified column, click that column's header (Category Count, IP Count, User Count, Site Count, Page Count, Object Count, or Time HH:MM:SS). Click the same column header again to sort records for that column in the reverse order.

Navigation tips

Back button

Click the Back button in the toolbar of the browser window to return to a previous page in the current report.

Record navigation field

The total number of records displays to the right of the Record navigation field, located above the rows of records:

This indicator helps you determine how long it will take to generate a report view or to print a report. If there are many records, you may wish to filter your results to reduce the time it will take to process the report.

The selected record is designated by the record number displayed in the Record navigation field, and by an arrow to the left of a record in the body of a report view.

To select another record, do any of the following:

- click the specified row to display the arrow preceding that record, and the record number in the Record navigation field.
- in the **Record** navigation field, enter a new record number in the white box between the arrow buttons to go to that record.

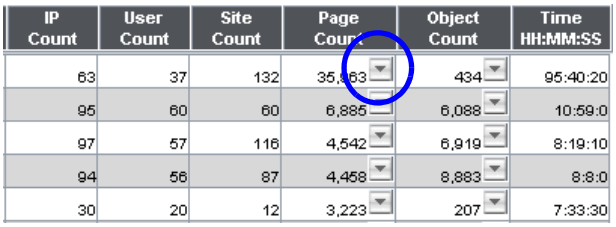
Downloaded from www.Manualslib.com manuals search engine

- in the Record navigation field, click any of the four arrow buttons to advance forward or backward through the list of records. In the order in which they display in the Record field, clicking these buttons moves you to the first record, the record prior to the selected record, the record following the selected record, and the last record.

Detail Drill Down Report navigation

By using the Summary Drill Down Report, the administrator should have narrowed the investigation to a specific category (e.g. “Pornography/Adult Content”) and a specific user name. The next step is to drill down into the detailed URL information to confirm the exact pages visited by the suspected policy violator.

To access the detail drill down report, click the arrow to the right of any record in the “Page Count” column of the Summary Drill Down Report:

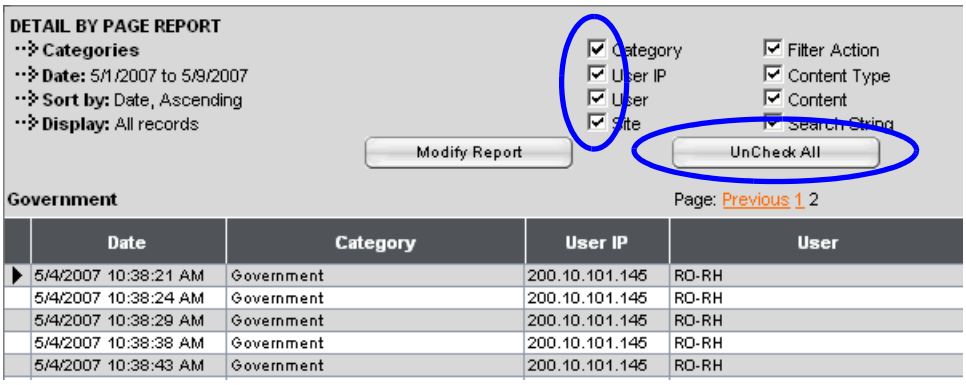


IP Count	User Count	Site Count	Page Count	Object Count	Time HH:MM:SS
63	37	132	35,663	434	95:40:20
95	60	60	6,885	6,088	10:59:0
97	57	116	4,542	6,919	8:19:10
94	56	87	4,458	8,883	8:8:0
30	20	12	3,223	207	7:33:30

Down arrow to the right of a record in a column

Report type columns

Below is a description of each column available in the detail drill down report view. The administrator can select which columns to display by selecting the check boxes or the “Check All”/“Uncheck All” button.



Checkboxes and UnCheck All / Check All button

- **Category** - the Category column includes the category name (e.g. “Alcohol”).
- **User IP** - the User IP column includes the IP address of the user’s machine (e.g. “200.10.101.80”).
- **User** - the User column includes any of the following information: username, user IP address, or the path and username (e.g. “logo\admin\jsmith”).
- **Site** - the Site column includes the URL the user attempted to access (e.g. “coors.com”).

Downloaded from www.Manualslib.com manuals search engine

- **Filter Action** - the Filter Action column displays the type of filter action used by the R3000 in creating the record: "Allowed", "Blocked", "Warn Blocked" (for the first warning page that displayed for the end user), "Warn Allowed" (for any subsequent warning page that displayed for the end user), "X-Strike", or "N/A" if the filter action was unclassified at the time the log file was created.
- **Content Type** - the Content Type column shows the method used by the R3000 in creating the record: “Search KW” (Search Engine Keyword), “URL KW” (URL Keyword), “URL”, “Wildcard”, “Https High” (HTTPS Filtering Level set at High), “X-strike” (X Strikes Blocking), “Pattern” (Proxy Pattern Blocking), “File Type”, “Https Medium” (HTTPS Filtering Level set at Medium), or “N/A” if the content was unclassified at the time the log file was created.
- **Content** - the Content column includes content type criteria used for determining the categorization of the record, or N/A if unclassified.
- **Search String** - the Search String column includes the full-length search string information the end user input into a Search Engine site text box. This is very useful in proving the intent of the user since the user manually types this into a search engine site (not a pop-up or auto-redirect).

To remove columns from the current report view:

- single column - click the checkbox for the specified column.
- all columns - click the **UnCheck All** button.

Page links

If more than one page of records was returned by the query, one or more Page numbers display(s) above the rows of records:

Click the page number to navigate to that page of records.

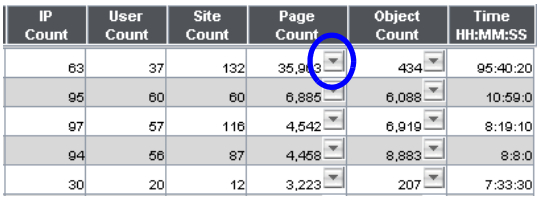
Downloaded from www.Manualslib.com manuals search engine

Evaluation steps

For the purpose of this evaluation, follow these steps to witness how the 8e6 Enterprise Reporter is best-in-class in terms of the extent of detailed page and object information it provides.

Step 1: Select a specific user by Category

If not already completed, select the page information drill down arrow to the right of any record in the “Page Count” column of the Summary Drill Down Report:

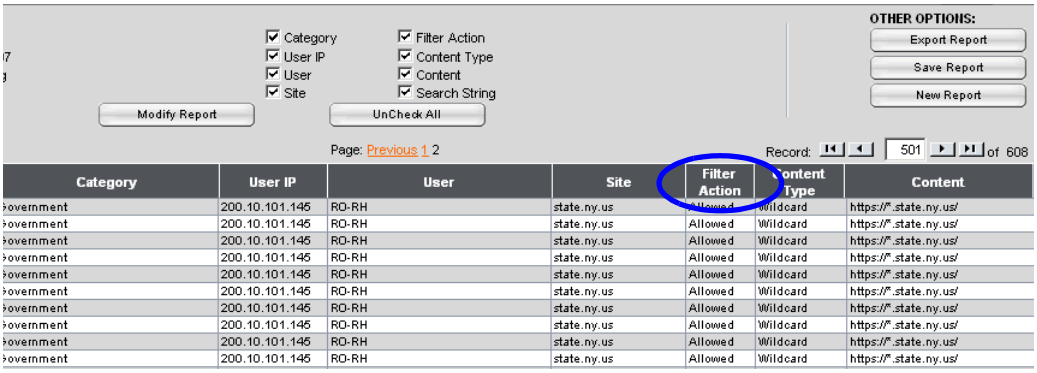


IP Count	User Count	Site Count	Page Count	Object Count	Time HH:MM:SS
63	37	132	35,9[illegible]	434	95:40:20
95	60	60	6,885	6,088	10:59:0
97	57	116	4,542	6,919	8:19:10
94	56	87	4,458	8,883	8:8:0
30	20	12	3,223	207	7:33:30

Page Count column, down arrow to the right

Step 2: Sort by “Filter Action” column

Clicking the “Filter Action” column header will sort all records by the type of filter action—whether the event was blocked, allowed or warned. Blocked searches will be highlighted in red font for easier detection.



Category, User IP, User, Site, Filter Action, Content Type, Content, Search String

OTHER OPTIONS: Export Report, Save Report, New Report

Modify Report | UnCheck All

Page: Previous 1 2 — Record: 501 of 608

Category	User IP	User	Site	Filter Action	Content Type	Content
Government	200.10.101.145	RO-RH	state.ny.us	Allowed	Wildcard	https://*.state.ny.us/
Government	200.10.101.145	RO-RH	state.ny.us	Allowed	Wildcard	https://*.state.ny.us/
Government	200.10.101.145	RO-RH	state.ny.us	Allowed	Wildcard	https://*.state.ny.us/
Government	200.10.101.145	RO-RH	state.ny.us	Allowed	Wildcard	https://*.state.ny.us/
Government	200.10.101.145	RO-RH	state.ny.us	Allowed	Wildcard	https://*.state.ny.us/
Government	200.10.101.145	RO-RH	state.ny.us	Allowed	Wildcard	https://*.state.ny.us/
Government	200.10.101.145	RO-RH	state.ny.us	Allowed	Wildcard	https://*.state.ny.us/
Government	200.10.101.145	RO-RH	state.ny.us	Allowed	Wildcard	https://*.state.ny.us/
Government	200.10.101.145	RO-RH	state.ny.us	Allowed	Wildcard	https://*.state.ny.us/

Filter Action column

Step 3: Full URL review

The full length URL of every Internet search by the users is listed in the “URL” column of the detail page information.

To view record data that displays truncated in a column, mouse over the column to view the entire string of data in the column for a given record:

Alcohol — Page: 1 2 Next — Record: 446 of 1000

Date	URL
7/14/2006 4:17:14 PM	http://www.budweiser.com/
7/14/2006 4:18:54 PM	http://www.beer.com/
7/14/2006 4:19:00 PM	http://www.budweiser.com/
7/14/2006 4:19:13 PM	http://www.beer.com/
7/14/2006 4:20:56 PM	http://www.budweiser.com/
7/17/2006 12:00:58 PM	http://www.coors.com/
7/17/2006 12:04:32 PM	http://www.whisky.com/
7/17/2006 12:13:25 PM	http://www.winespectator.com/
7/17/2006 12:13:25 PM	http://www.winespectator.com/Wine/Home/
7/17/2006 12:13:27 PM	http://www.winespectator.com/Wine/Help/Page_Error/1%p39_23%+l_s2=6%13s.html
7/17/2006 1:35:14 PM	http://coors.com/
7/17/2006 1:35:21 PM	http://www.coors.com/
7/17/2006 1:35:39 PM	http://jimbeam.com/

Mouse over to view full URL

Downloaded from www.Manualslib.com manuals search engine

Click the URL link to launch the actual Web site viewed by the user to verify the content that was accessed.

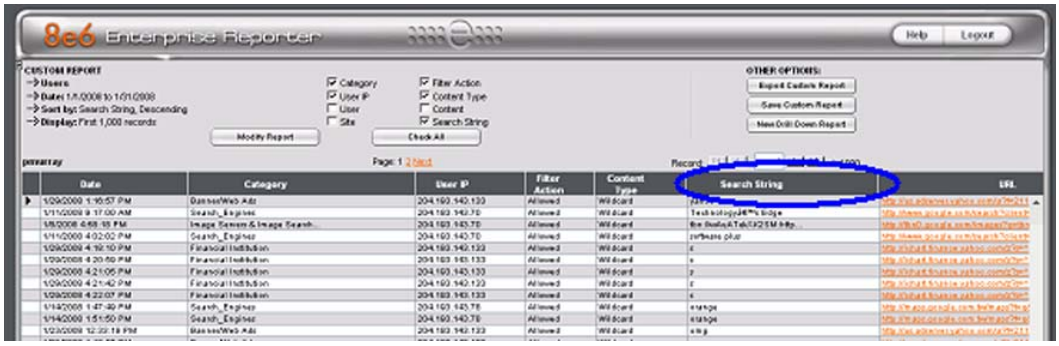
Step 4: Sort by "Content Type"

Sort by the column labeled "Content Type" by clicking that column header. This will sort all records by the search type filtered on the R3000 Internet Filter. For example, "**URL**" indicates a page request was blocked or allowed based on the status of that URL in the 8e6 category library and "**Search KW**" indicates a user typed in a prohibited word into a search engine text box. One of 8e6 Technologies' differentiators is "**Proxy Pattern Blocking**," which will show up in the "Content Type" section if an Internet proxy site was blocked by 8e6's proprietary proxy signature detection.

After reviewing a suspected policy violator's Internet activity in the Detail Drill Down Report, the administrator will have firm evidence on the user's *intent*, which is critical forensic information to have in the event the investigation moves to the disciplinary phase.

Step 5: Sort by "Search String"

Sort by the column labeled "Search String" by clicking that column header. This will sort all records alphabetically for results that include search string information. Search string content includes the actual text typed into a search engine text box on popular search engine sites such as Google, Yahoo, Ask.com and MSN. For example, if the end user typed in "recipes for chicken breast" in a search engine request, that entire string will appear in this column, not simply the blocked keywords within the request. This depth of detail helps clarify the intent of the end user, which helps tremendously in investigations.



Search String column

In the next section, this guide will go through the final step in a typical investigation—creating a **Specific User Custom Report**.

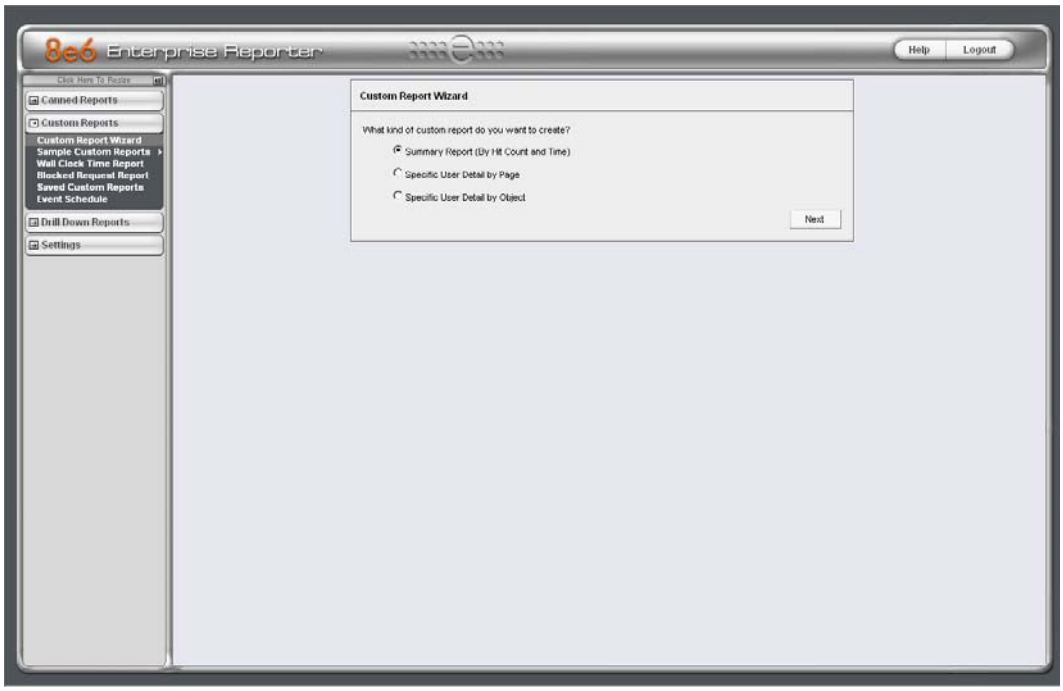
Downloaded from www.Manualslib.com manuals search engine

Create a Custom Report for a specific user

After reviewing the detail drill down report, if the administrator is confident that an individual has violated the Internet Acceptable Use Policy (AUP), the most common step to take next is to run a custom report for this specific individual that covers a greater time period period. While there are several ways to accomplish this in the Enterprise Reporter, this guide will focus on the most commonly used method—the **Custom Report Wizard**.

How to use the Custom Report Wizard

The Custom Report Wizard option provides an intuitive setup process for generating custom reports for one time use, or for recurrence at scheduled time periods. The “Custom Report Wizard” option is available from the “Custom Reports” menu, accessed from the navigation panel:



Custom Report Wizard window

Generate a new Custom Report

To generate a specific user custom report:

1. Select radio button next to “**Specific User Detail by Page**” and click the “**Next**” button.
2. Specify the date and time range for the query:
   - At the **From Date** field, specify the start of the date range by making a selection from any of the pull-down menus for month (1-12), day (1-31), or year (1998-2009). (For evaluation purposes, select the date the Enterprise Reporter was installed to gather the most information available.)
   - At the **To Date** field, specify the end of the date range by making a selection from any of the pull-down menus for month (1-12), day (1-31), or year (1998-2009).

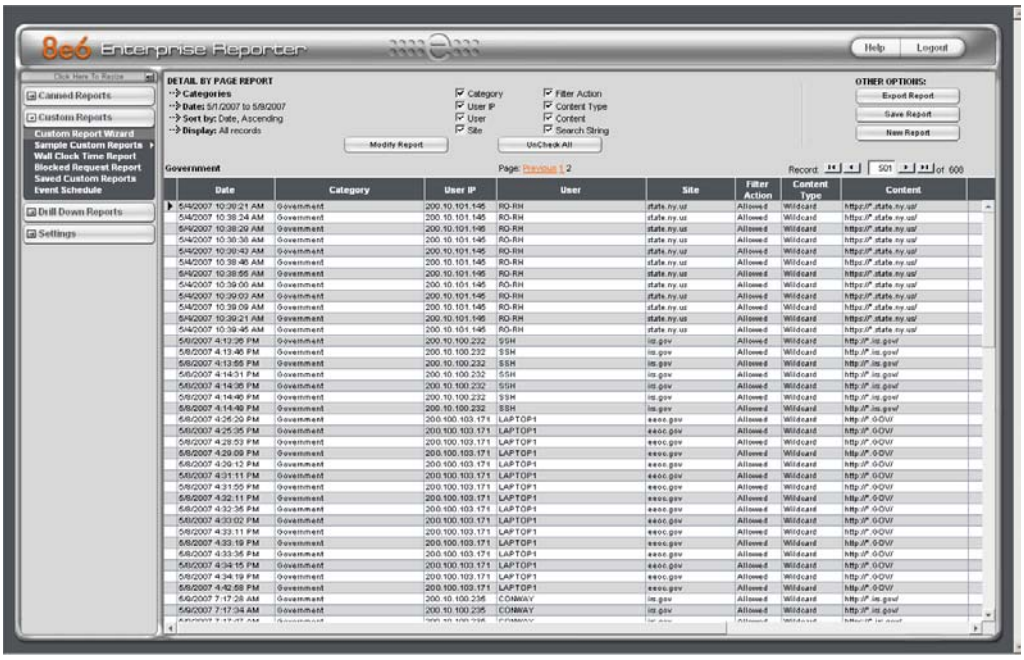
Downloaded from www.Manualslib.com manuals search engine

- At the **From Time** field, specify the start of the time range by making a selection from any of the pull-down menus for the hour (1-12), minute (00-59), or AM or PM.
- At the **To Time** field, specify the end of the time range by making a selection from any of the pull-down menus for the hour (1-12), minute (00-59), or AM or PM.

3. Specify the type of query you wish to perform (Category, User IP, Username, Site):

   - **Category** - to perform a query on activity within a specific filter category, make a selection from the filter categories in the pull-down menu. Category items are set up under the Category Descriptions option from the Settings menu. (For evaluation purposes, leave this section blank to gather the most information about the user's activity.)
   - **User IP** - to perform a query on the activity of a specific machine, enter the IP address of the machine (e.g. "200.10.100.174"). (For evaluation purposes, leave this section blank to gather the most information about the user's activity.)
   - **Username** - to perform a query on the activity of a specific user, enter the username (e.g. "tjohnson"). You can use the "%" character before and after a partial name to do a wildcard search (e.g. %johnson%). (For evaluation purposes, select a user name with frequent Internet activity to ensure the report generates some data.)
   - **Site** - to perform a query on activity at a specific Web site visited by users, enter the domain or site address (e.g. "yahoo.com" or "icq.com"). (For evaluation purposes, leave this section blank to gather the most information about the user's activity.)

4. After defining items in steps 2 and 3, click the "**View Drill Down Results**" button to begin generating the report.



Custom Report Wizard Specific User Detail by Page report

Downloaded from www.Manualslib.com manuals search engine

***NOTE**: As the report is generating, a window displays on the screen providing status on which stage of the report process is underway.*

When completely generated, the specific user report displays in the view pane. This report has the same format as the detail drill down report discussed earlier.

The custom report view can be exported, saved, and/or scheduled to run at a specified time.

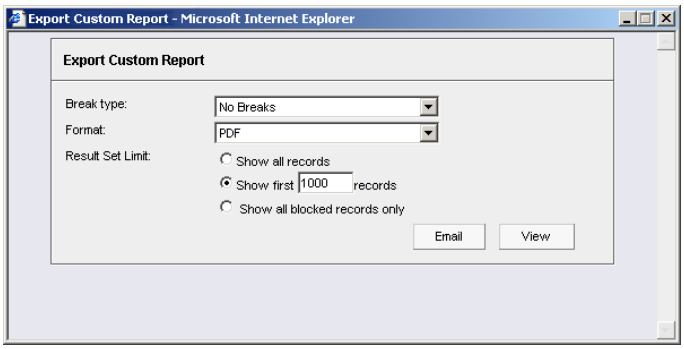
***NOTE**: See 'Export a Custom Report' for information on exporting a report view. See ''Schedule a report to run' for information on how to schedule a report to run at a specified time.*

Next steps for documenting, monitoring specific user activity

Once the specific user report has been generated, the administrator can choose to export and save the report for documenting a case against the policy violator and can also schedule the report to run in the future to monitor this individual on an ongoing basis.

Export a Custom Report

1. Click the **Export Report** button to open the Export Custom Report pop-up box:



Export Custom Report option (Detail report)

***NOTE**: Information on using the fields in this pop-up box can be found in the 'Report fields' sub-section.*

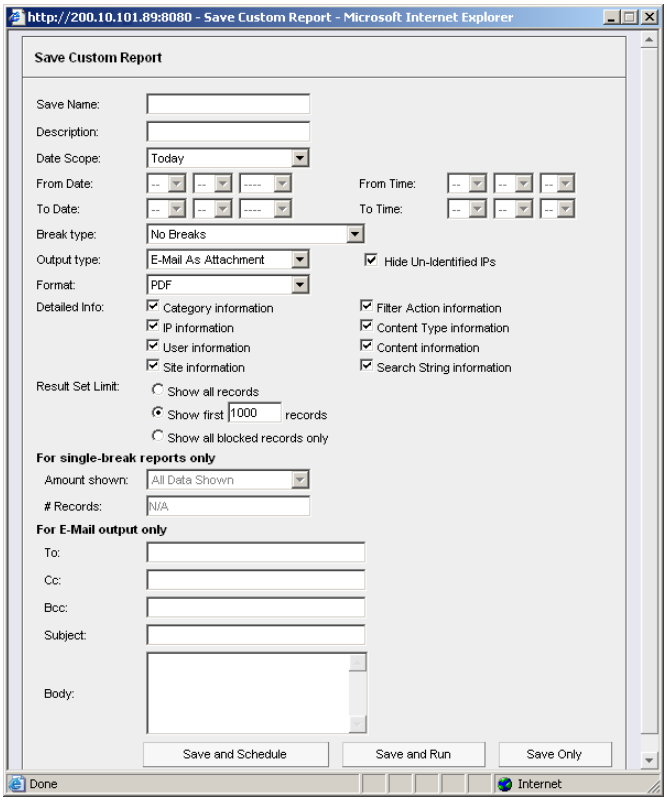
2. Modify the Break type and Format, and specify the number of records to be included in the report view.
3. After making selections and/or entries in all fields, click the **Email** or **View** button to close this pop-up box and to export the data in the specified file format.

***NOTE**: Information on using the buttons this pop-up box can be found in the 'Other Summary Report Tools' sub-section.*

Downloaded from www.Manualslib.com manuals search engine

Save a Detail Custom Report

1. Click the **Save Report** button to open the Save Custom Report pop-up box:



Save Custom Report option (Detail report)

2. In the **Save Name** field, enter a name for the report. This name will display in the Report Name pull-down menu in the Saved Custom Reports option accessible via the Custom Reports menu.
3. In the **Description** field, enter the report description. This description will display in the Report Description field in the Saved Custom Reports option accessible via the Custom Reports menu.
4. The date scope for the current report view displays in the From Date and To Date fields. If you wish to change the date scope, make a selection from the following choices in the **Date Scope** pull-down menu: “Today”, “Month to Date”, “Monthly", “Year to Date", “Daily", “Yesterday", “Month to Yesterday", “Year to Yesterday", “Last Week", “Last Weekend", “Current Week", “Last Month”. (For evaluation purposes select “Last Week”.)
5. Choose the break type, output type and format:
   - **Break type** - available selections are based on the type of report generated. There are no break types available for specific user reports.
   - **Output type** - choose either “E-Mail As Attachment”, or “E-Mail As Link”.
   - **Format** - selections include: “MS-DOS Text”, “PDF”, “Rich Text Format”, “HTML”, “Comma-Delimited Text”, and “Excel (English)”.
6. The “Hide Un-Identified IPs” checkbox is de-selected by default if the checkbox by this same name was deselected in the Options window. To change the selection in this field, click the “Hide Un-Identified IPs” checkbox to remove—or

Downloaded from www.Manualslib.com manuals search engine

add—a check mark in the checkbox. By entering a check mark in this checkbox, activity on machines not assigned to specific end users will not be included in report views. Changing this selection will not affect the setting previously saved in the Options window. (For purposes of this evaluation, leave this checkbox de-selected.)

7. To include the specified column in the report, click any of the following check-boxes listed below. (For purposes of this evaluation, select all checkboxes.)
   - **Category information** - this column will include the category name (e.g. “Alcohol”) for each record.
   - **IP information** - this column will include the IP address of the machine (e.g. “200.10.101.80”) for each record.
   - **User information** - this column will include the path of the username (e.g. LOGO\Admin\JSmith”) for each record.
   - **Site information** - this column will include the URL of the Web site visited by the user (e.g. “coors.com”) for each record.
   - **Filter Action information** - this column will include the type of filter action used by the R3000 in creating the record: "Allowed", "Blocked", "Warn Blocked" (for the first warning page that displayed for the end user), "Warn Allowed" (for any subsequent warning page that displayed for the end user), "X-Strike", or "N/A" if the filter action was unclassified at the time the log file was created.
   - **Content Type information** - this column will include the method used by the R3000 in creating the record: “Search KW” (Search Engine Keyword), “URL KW” (URL Keyword), “URL”, “Wildcard”, “Https High” (HTTPS Filtering Level set at High), “X-strike” (X Strikes Blocking), “Pattern” (Proxy Pattern Blocking), or “N/A” if the content was unclassified at the time the log file was created.
   - **Content information** - this column will include criteria used for determining the categorization of the record, or “N/A” if unclassified.
   - **Search String information** - this column will include the full search string the end user typed into a search engine text box. This column displays pertinent information only if the Search Engine Reporting option is enabled in the Optional Features screen of the Administrator interface.
8. In the **Result Set Limit** field, specify the records to be included in the report view. (For purposes of this evaluation, specify “Show first 100 records.”
9. In the **For E-Mail output only** field, fill in the fields for emailing the report: “To”, “Cc”, “Bcc”, “Subject”, and “Body”.
10. Click **Save Only** to save your selections and entries for the custom report, and to close this pop-up box.

***NOTE**: See ‘Schedule a report to run’ for information on how to schedule a report to run at a specified time.*

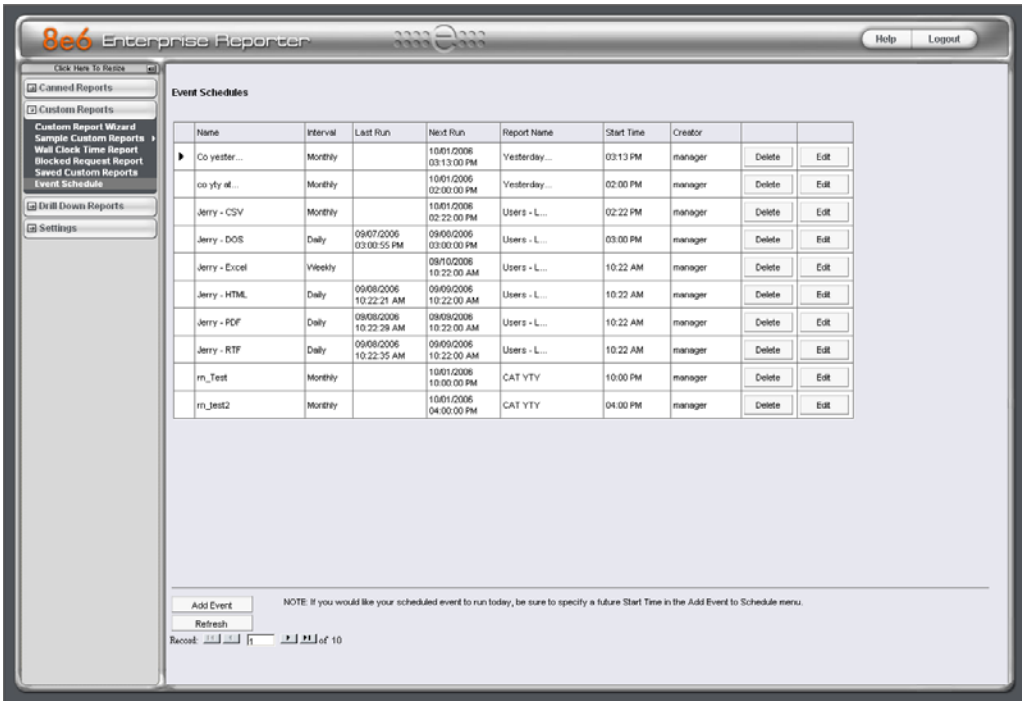
Downloaded from www.Manualslib.com manuals search engine

Schedule a report to run

Once a report view has been saved, it can be scheduled to run at a designated time.

To schedule a report to run:

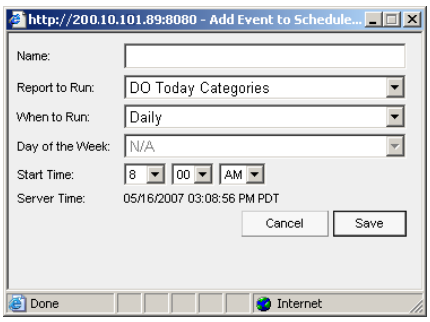
1. Go to the Settings menu in the navigation panel and select Event Schedule. The Event Schedule option is used for maintaining a schedule for generating a customized report.



Event Schedule window (administrator login)

If logged in as the administrator, all scheduled events display. If logged in as a manager, only the events scheduled by that manager login ID display. If the Web Client Scheduler is turned off, the message “To view event schedules, please enable Web Client scheduler using ER Admin GUI.” displays in place of scheduled events.

2. In the Event Schedule window, click the **Add Event** button to open the Add Event to Schedule dialog box:



Add an Event

3. Enter a **Name** for the event.

Downloaded from www.Manualslib.com manuals search engine

4. Select the **Report to Run** from the pull-down menu.
5. Select the frequency **When to Run** from the pull-down menu ("Daily", "Weekly", or "Monthly").

   If Weekly, specify the **Day of the Week** from the pull-down menu (Sunday - Saturday).
6. Select the **Start Time** for the report: 1 - 12 for the hour, 00 - 59 for the minute, and AM or PM.

***NOTE**: The default Start Time is 8:00 AM. If you wish to run a report today and this time has already passed, be sure to select a future time.*

***TIP**: Click Cancel to return to the Event Schedules window without saving your edits.*

7. Click **Save** to add the scheduled event. The custom report will now be sent automatically at the pre-defined time on an ongoing basis until the administrator deletes the scheduled event.

   By saving and scheduling this custom specific user report, the administrator will be able to conveniently monitor policy violators in the future and use these reports in any disciplinary action that may result.

Downloaded from www.Manualslib.com manuals search engine

Appendix A: Samples of Commonly Used Reports

Though this Evaluation Guide is primarily designed to lead the evaluator through the process of an investigation, there are many other useful features to explore in the Enterprise Reporter. Below is a summary of some of the other custom reports an administrator can create and have automatically emailed on a regular basis in order to be kept up to date on Internet threats arising from within the organization.

8e6 has created 10 different sample report formats to help first time users understand the various types of reports available in the Enterprise Reporter. For purposes of this Evaluation Guide, only three of the 10 are described in detail below. A complete description of all other sample reports is available in the **Enterprise Reporter Web Client User Guide**.

How to generate a Sample Custom Report

1. Choose Sample Custom Reports from the Custom Reports menu, and then click one of the following available selections to open a separate browser window containing the generated canned report in the PDF format:
   - **Top 20 Categories by Page Count**
   - **Top 20 IPs by Category/IP**
   - **Top 20 Users by Category/User**
   - **Top 20 Users by Page Count**
   - **Top 20 Categories by User/Category**
   - **Top 20 Sites by User/Site**
   - **By User/Category/Site**
   - **Top 20 Sites by Category/Site**
   - **By Category/Site/IP**
   - **By Category/User/Site**
2. From the open PDF file, the canned report can be exported in some of the following ways:
   - print the report - click the print icon to open the Print dialog box, and proceed with standard print procedures.
   - save the report - click the save icon to open the Save a Copy dialog box, and proceed with standard save procedures.
3. Click the “X” in the upper right corner of the report window to close it.

Downloaded from www.Manualslib.com manuals search engine

Report format

For each report, the header of the reports contain the following information:

- **Sort Order: Page Count, descending**
- **From:** / **To:** today's date displays
- the name of the report displays

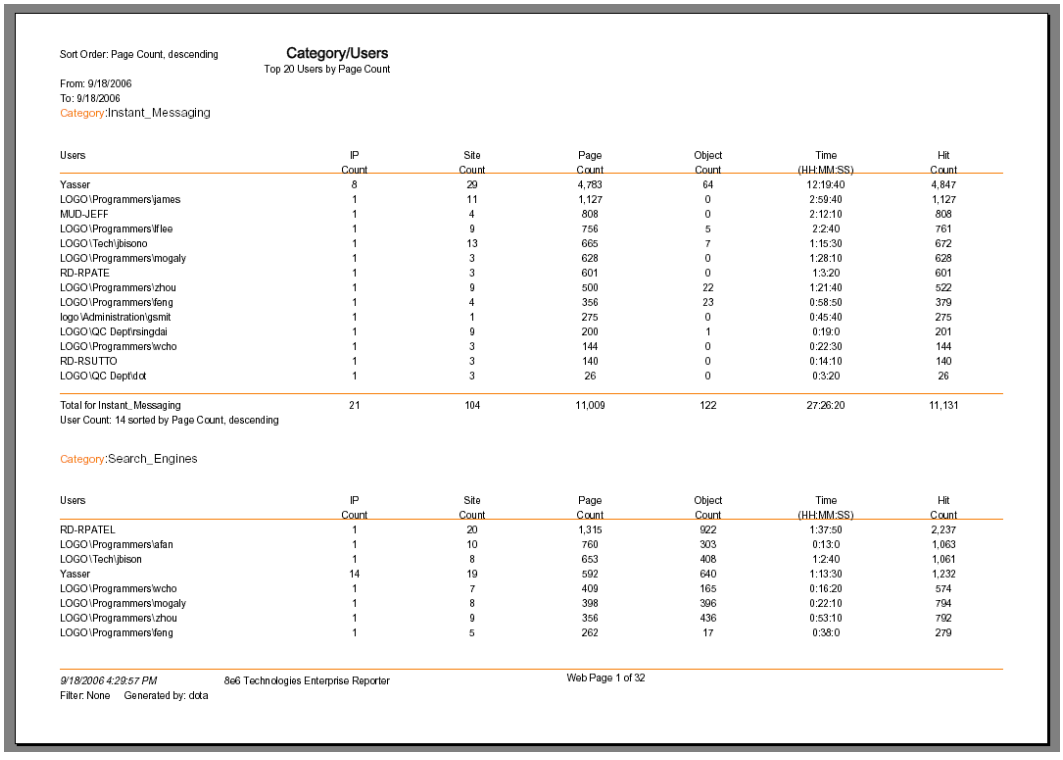
The footer of the reports contain the following information:

- today's date (MM/DD/YYYY) and time (HH:MM:SS AM/PM) the report was generated
- **Page** number
- **Filter: None**
- Generated by: manager's login ID

Examples of available Sample Custom Reports

Sample Report 1: "Top 20 Users by Category/User"

This report shows the top 20 users for each of the categories in the 8e6 library. This is a useful tool to quickly scan for excessive use of any category.



Sort Order: Page Count, descending

Category/Users
Top 20 Users by Page Count

From: 9/18/2006
To: 9/18/2006
Category:Instant_Messaging

Users	IP Count	Site Count	Page Count	Object Count	Time (HH:MM:SS)	Hit Count
Yasser	8	29	4,783	64	12:19:40	4,847
LOGO\Programmers\james	1	11	1,127	0	2:59:40	1,127
MUD-JEFF	1	4	808	0	2:12:10	808
LOGO\Programmers\lflee	1	9	756	5	2:2:40	761
LOGO\Tech\jbisono	1	13	665	7	1:15:30	672
LOGO\Programmers\mogaly	1	3	628	0	1:28:10	628
RD-RPATE	1	3	601	0	1:3:20	601
LOGO\Programmers\zhou	1	9	500	22	1:21:40	522
LOGO\Programmers\feng	1	4	356	23	0:58:50	379
logo\Administration\gsmit	1	1	275	0	0:45:40	275
LOGO\QC Dept\rsingdai	1	9	200	1	0:19:0	201
LOGO\Programmers\wcho	1	3	144	0	0:22:30	144
RD-RSUTTO	1	3	140	0	0:14:10	140
LOGO\QC Dept\dot	1	3	26	0	0:3:20	26
Total for Instant_Messaging	21	104	11,009	122	27:26:20	11,131

User Count: 14 sorted by Page Count, descending

Category:Search_Engines

Users	IP Count	Site Count	Page Count	Object Count	Time (HH:MM:SS)	Hit Count
RD-RPATEL	1	20	1,315	922	1:37:50	2,237
LOGO\Programmers\afan	1	10	760	303	0:13:0	1,063
LOGO\Tech\jbison	1	8	653	408	1:2:40	1,061
Yasser	14	19	592	640	1:13:30	1,232
LOGO\Programmers\wcho	1	7	409	165	0:16:20	574
LOGO\Programmers\mogaly	1	8	398	396	0:22:10	794
LOGO\Programmers\zhou	1	9	356	436	0:53:10	792
LOGO\Programmers\feng	1	5	262	17	0:38:0	279

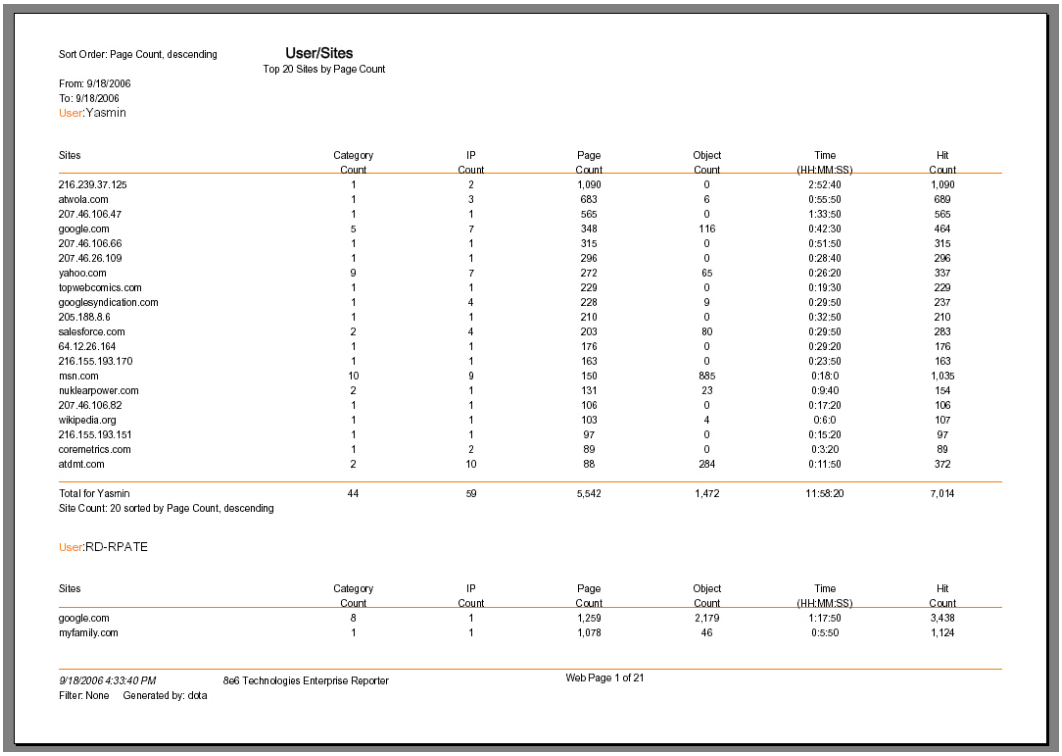
9/18/2006 4:29:57 PM 8e6 Technologies Enterprise Reporter Web Page 1 of 32
Filter: None Generated by: dota

Sample Category/Users report

Downloaded from www.Manualslib.com manuals search engine

Sample Report 2: "Top 20 Sites by User/Site"

This report will document the top 20 sites visited for every user in the organization. This is a useful tool in monitoring the high level Web activity of users, and can help fine-tune sites the administrator allows users to access.



Sort Order: Page Count, descending

User/Sites
Top 20 Sites by Page Count

From: 9/18/2006
To: 9/18/2006
User:Yasmin

Sites	Category Count	IP Count	Page Count	Object Count	Time (HH:MM:SS)	Hit Count
216.239.37.125	1	2	1,090	0	2:52:40	1,090
atwola.com	1	3	683	6	0:55:50	689
207.46.106.47	1	1	565	0	1:33:50	565
google.com	5	7	348	116	0:42:30	464
207.46.106.66	1	1	315	0	0:51:50	315
207.46.26.109	1	1	296	0	0:28:40	296
yahoo.com	9	7	272	65	0:26:20	337
topwebcomics.com	1	1	229	0	0:19:30	229
googlesyndication.com	1	4	228	9	0:29:50	237
205.188.8.6	1	1	210	0	0:32:50	210
salesforce.com	2	4	203	80	0:29:50	283
64.12.26.164	1	1	176	0	0:29:20	176
216.155.193.170	1	1	163	0	0:23:50	163
msn.com	10	9	150	885	0:18:0	1,035
nuklearpower.com	2	1	131	23	0:9:40	154
207.46.106.82	1	1	106	0	0:17:20	106
wikipedia.org	1	1	103	4	0:6:0	107
216.155.193.151	1	1	97	0	0:15:20	97
coremetrics.com	1	2	89	0	0:3:20	89
atdmt.com	2	10	88	284	0:11:50	372
Total for Yasmin	44	59	5,542	1,472	11:58:20	7,014

Site Count: 20 sorted by Page Count, descending

User:RD-RPATE

Sites	Category Count	IP Count	Page Count	Object Count	Time (HH:MM:SS)	Hit Count
google.com	8	1	1,259	2,179	1:17:50	3,438
myfamily.com	1	1	1,078	46	0:5:50	1,124

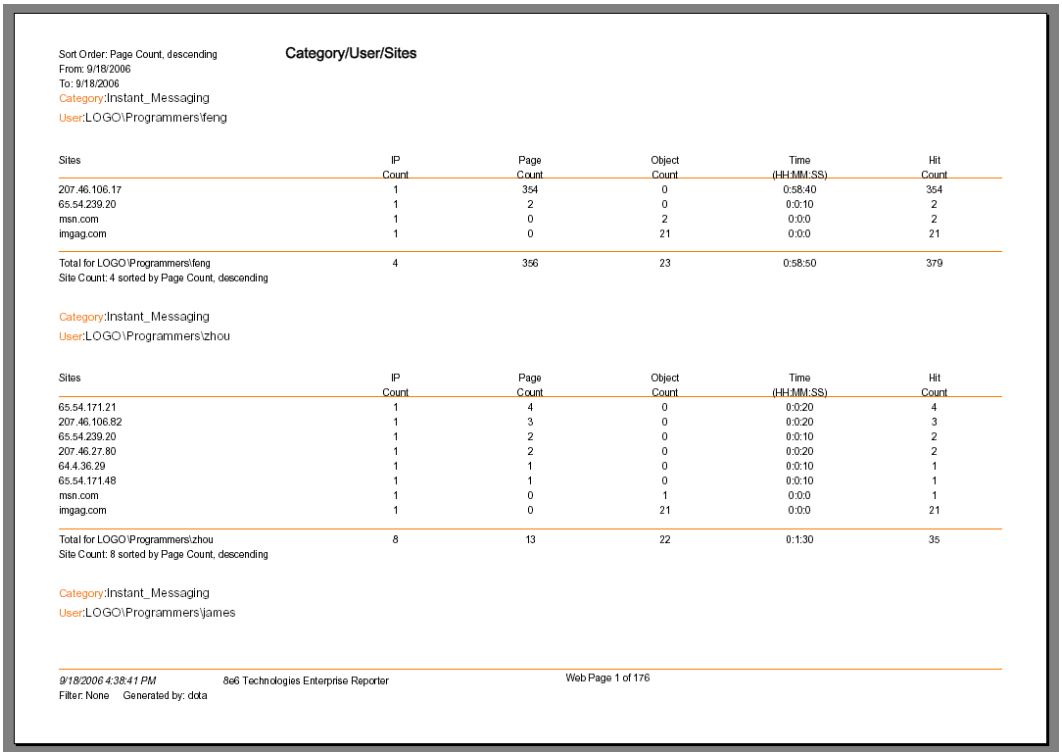
9/18/2006 4:33:40 PM 8e6 Technologies Enterprise Reporter Web Page 1 of 21
Filter: None Generated by: dota

Sample User/Sites report

Downloaded from www.Manualslib.com manuals search engine

Sample Report 3: "By Category/User/Site"

This is an example of a triple break report that shows all activity on the network, broken out by category, then user, and then site. This is a useful report if the administrator is looking for an all-encompassing view of Internet activity within the organization. However, please note that this is usually a very lengthy report since it captures all user information by site.



Sort Order: Page Count, descending
From: 9/18/2006
To: 9/18/2006

Category/User/Sites

Category:Instant_Messaging
User:LOGO\Programmers\feng

Sites	IP Count	Page Count	Object Count	Time (HH:MM:SS)	Hit Count
207.46.106.17	1	354	0	0:58:40	354
65.54.239.20	1	2	0	0:0:10	2
msn.com	1	0	2	0:0:0	2
imgag.com	1	0	21	0:0:0	21
Total for LOGO\Programmers\feng	4	356	23	0:58:50	379

Site Count: 4 sorted by Page Count, descending

Category:Instant_Messaging
User:LOGO\Programmers\zhou

Sites	IP Count	Page Count	Object Count	Time (HH:MM:SS)	Hit Count
65.54.171.21	1	4	0	0:0:20	4
207.46.106.82	1	3	0	0:0:20	3
65.54.239.20	1	2	0	0:0:10	2
207.46.27.80	1	2	0	0:0:20	2
64.4.36.29	1	1	0	0:0:10	1
65.54.171.48	1	1	0	0:0:10	1
msn.com	1	0	1	0:0:0	1
imgag.com	1	0	21	0:0:0	21
Total for LOGO\Programmers\zhou	8	13	22	0:1:30	35

Site Count: 8 sorted by Page Count, descending

Category:Instant_Messaging
User:LOGO\Programmers\james

9/18/2006 4:38:41 PM 8e6 Technologies Enterprise Reporter Web Page 1 of 176
Filter: None Generated by: dota

Sample Category/User/Sites report

Downloaded from www.Manualslib.com manuals search engine

Appendix B: Export and Save Summary Reports

The Enterprise Reporter has a variety of different reporting options. In a fashion similar to the Specific User Report creation process described in the sample investigation earlier in this guide, administrators can also create custom reports from a Summary Drill Down Report view. Summary Custom Reports can be set up to be automatically emailed to the administrator on a regular basis in a variety of formats (e.g. PDF, Excel, etc.). Follow the steps below on how to export and save these types of custom reports.

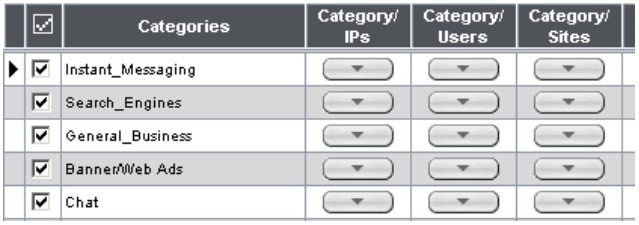
Record exportation tip

Step 1: Select records to be exported

In the report view, each record is preceded by a checkbox that is populated (selected) by default.

When exporting a report, only selected records are included. To de-select a record, click the checkbox to remove the check mark from the checkbox.

To de-select all records, click the checkbox in the column header. Clicking the checkbox in the column header again reselects all records.



Step 2: Use header buttons for report customization

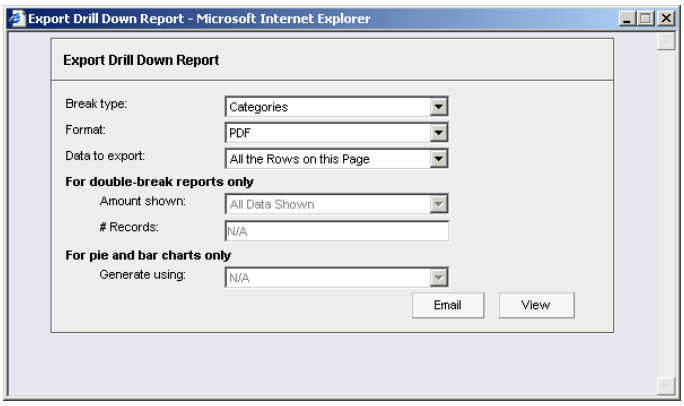
Clicking one of the buttons at the top of the summary report view opens a pop-up box that lets you customize the current report view. The following buttons are available:

- **New Report** - this option lets you generate a drill down report view for a date range other than the current (default) date.
- **Modify Report** - this option lets you modify the current report view by doing any of the following: specify the maximum number of records to be included other than the number entered in Default Options; perform a search for specified text, or sort the report in ascending or descending order by a specified column.
- **Export Report** - this option lets you email, print, or view the current report view in the specified output format.
- **Save Report** - this option lets you save the current report view so a report using these customizations can be run again later at a designated time.
- **Set Result Limit** - this option lets you specify the maximum number of records to be included in the report view, instead of the default number (entered in Default Options).

Downloaded from www.Manualslib.com manuals search engine

Step 3: Export a Summary Drill Down Report

1. Click the **Export Report** button to open the Export Drill Down Report pop-up box:



Export Drill Down Report option (Summary report)

***NOTE**: Information on using the fields in this pop-up box can be found in the 'Report fields' sub-section.*

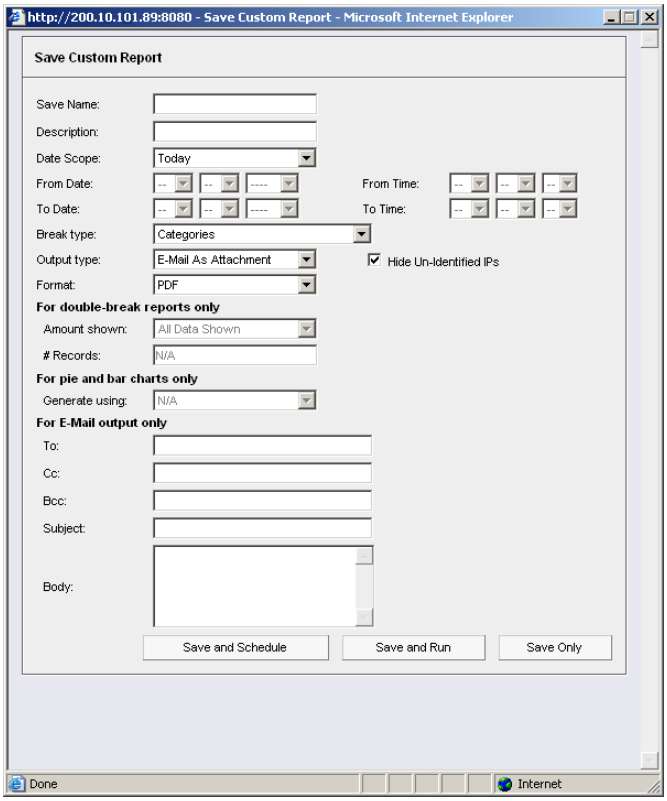
2. At the **Data to export** field, select the amount of data to be exported from the pull-down menu: "All the Rows on this Page", or "Only the Selected Rows on this Page". The second selection is available only if some of the records in the report view were de-selected.
3. After making selections and/or entries in all fields, click the **Email** or **View** button to close this pop-up box and to export the data in the specified file format.

***NOTE**: Information on using the buttons this pop-up box can be found in the 'Methods for exporting a Drill Down Report' sub-section.*

Downloaded from www.Manualslib.com manuals search engine

How to save a Summary Drill Down Report

1. Click the **Save Report** button to open the Save Custom Report pop-up box:



Save Custom Report option (Summary report)

2. In the **Save Name** field, enter a name for the report. This name will display in the Report Name pull-down menu in the Saved Custom Reports option accessible via the Custom Reports menu.

***TIP**: The Copy (Ctrl+C) and Paste (Ctrl+V) functions can be used in the fields in the Save Custom Report pop-up box.*

3. In the **Description** field, enter the report description. This description will display in the Report Description field in the Saved Custom Reports option accessible via the Custom Reports menu.

4. The date scope for the current report view displays in the From Date and To Date fields. If you wish to change the date scope, make a selection from the following choices in the **Date Scope** pull-down menu: “Today”, “Month to Date”, “Monthly", “Year to Date", “Daily", “Yesterday", “Month to Yesterday", “Year to Yesterday", “Last Week", “Last Weekend", “Current Week", “Last Month”.

   - The From Date and To Date fields become unavailable if one of the following selections is made: “Today”, “Month to Date”, “Year to Date", “Yesterday", “Month to Yesterday", “Year to Yesterday", “Last Week", “Last Weekend", “Current Week", “Last Month”.
   - If Monthly is selected, in the **From Date** and **To Date** fields, make a selection for the month (1-12), and year (1998-2009).
   - If Daily is selected, in the **From Date** and **To Date** fields, make a selection for the month (1-12), day (1-31), and year (1998-2009).

Downloaded from www.Manualslib.com manuals search engine

5. Choose the break type, output type and format:
   - **Break type** - available selections are based on the type of report generated. There are no break types available for specific user reports.
   - **Output type** - choose either “E-Mail As Attachment”, or “E-Mail As Link”.
   - **Format** - selections include: “MS-DOS Text”, “PDF”, “Rich Text Format”, “HTML”, “Comma-Delimited Text”, and “Excel (English)”.
6. The “Hide Un-Identified IPs” checkbox is de-selected by default if the checkbox by this same name was deselected in the Options window.

***NOTE**: The Options window is accessible via Default Options in the Settings menu. See the Default Options sub-section in Chapter 2: Customizing the Client of the Enterprise Reporter Web Client User Guide for more information about the Hide Un-Identified IPs option.*

To change the selection in this field, click the “Hide Un-Identified IPs” checkbox to remove—or add—a check mark in the checkbox. By entering a check mark in this checkbox, activity on machines not assigned to specific end users will not be included in report views. Changing this selection will not affect the setting previously saved in the Options window.

7. If pertinent, make a selection for additional reporting options:
   - **For double-break reports only** - specify the top count option to be used.
   - **For pie and bar charts only** - specify the count column sort option to be used.

***NOTE**: Information on using the fields not detailed in this pop-up box can be found in the ‘Report fields’ sub-section.*

8. In the **For E-Mail output only** field, fill in the fields for emailing the report: “To”, “Cc”, “Bcc”, “Subject”, and “Body”.
9. Click **Save Only** to save your selections and entries for the custom report, and to close this pop-up box. Most of the captured information is available for modification in the Saved Custom Reports option accessible via the Custom Reports menu.

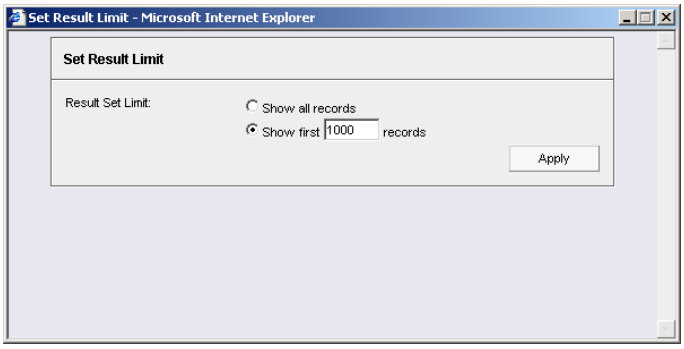
***NOTE**: See ‘Schedule a report to run’ for information on how to schedule a report to run at a specified time.*

Downloaded from www.Manualslib.com manuals search engine

Other Summary Report tools

Set Result Limit

1. Click the **Set Result Limit** button to open the Set Result Limit pop-up box:



Set Result Limit option (Summary report only)

2. Indicate the **Result Set Limit** by selecting the appropriate radio button:
   - **Show all records** - Click this radio button to include all records returned by the report query.
   - **Show first** 'X' **records** - Click this radio button to only include the first set of records returned by the report query.
3. Indicate the number of records to be included in a set by making an entry in the blank field, represented here by the 'X'.
4. Click **Apply** to apply your settings in the current report view and to close this pop-up box.

Report fields

Type field

The Type field is used for specifying the report type by which the generated report view will be sorted. This field is available in the Drill Down Report pop-up box via the New Report option, and in the Single User Group window.

At the **Type** field, make a selection from the pull-down menu for one of the available report types: "Categories", "IPs", "Users", "Sites", "Category Groups", "User Groups", and the current report format displayed.

Date Scope and Date fields

The Date Scope field is used for specifying the period of time to be included in the generated report view. Depending on the scope selected, the From Date and To Date fields are used in conjunction with this field. These fields are available in the Drill Down Report pop-up box via the New Report option, in the Single User Group window, and in the Save Custom Report pop-up box via the Save Report option.

At the **Date Scope** field, make a selection from the pull down menu for the time frame you wish to use in your query: "Today", "Month to Date", "Monthly", "Year to Date", "Daily", "Yesterday", "Month to Yesterday", "Year to Yesterday", "Last

Downloaded from www.Manualslib.com manuals search engine

Week", “Last Weekend", “Current Week", “Last Month”. Reports can be run for any data saved in the ER Server’s memory.

- **Today** - this option generates the report view for today only, if logs from the Web access logging device have been received and processed.
- **Month to Date** - this option generates the report view for the range of days that includes the first day of the current month through today.
- **Monthly** - selecting this option activates the **From Date** and **To Date** pull-down menus where you specify the range of months (1-12) and/or years (1998-2009).
- **Year to Date** - this option generates the report view for the range of days that includes the first day of the current year through today.
- **Daily** - selecting this option activates the **From Date** and **To Date** pull-down menus where you specify the range of months (1-12), days (1-31), and/or years (1998-2009).

  The generated report view includes data for the specified days only, if the data for these days are stored on the Server.
- **Yesterday** - this option generates the report view for yesterday only.
- **Month to Yesterday** - this option generates the report view for the range of days that includes the first day of the current month through yesterday.
- **Year to Yesterday** - this option generates the report view for the range of days that includes the first day of the current year through yesterday.
- **Last Week** - this option generates the report view for all days in the past week, beginning with Sunday and ending with Saturday.
- **Last Weekend** - this option generates the report view for the past Saturday and Sunday.
- **Current Week** - this option generates the report view for today and all previous days in the current week, beginning with Sunday and ending with Saturday.
- **Last Month** - this option generates the report view for all days within the past month.

Display and # Records fields

The Display and # Records fields are used for specifying the number of records from the query you wish to include in the report view, and how these records will be sorted. These fields are available in the Drill Down Report pop-up box via the Modify Report option, and in the Advance Options portion of the New Report option and Single User Group window.

At the **Display** field, make a selection from the pull-down menu for the records to be shown on the screen: “All Data Shown”, “Top Category Count”, “Top IP Count”, “Top User Count”, “Top Site Count”, “Top Page Count”, “Top Object Count”, “Top Time”, “Top Hit Count”.

In the **# Records** field, “N/A” displays grayed-out if “All Data Shown” was selected at the Display field. If any other selection was made at the previous field, the default number saved in the Options window displays in this field. Enter the maximum number of top records to be included in the query.

Downloaded from www.Manualslib.com manuals search engine

***NOTE**: The Default Top Value entry in the Default Options window is accessible via Default Options in the Settings menu. See the Default Options sub-section in Chapter 2: Customizing the Client of the Enterprise Reporter Web Client User Guide for more information about the Default Top Value.*

Search and Filter String fields

The Search and Filter String fields are used for specifying search criteria in the current summary report view.

At the **Search** field, make a selection from the pull-down menu for the search term to be used: “None”, “Contains”, “Starts with”, “Ends with”.

In the **Filter String** field, “N/A” displays greyed-out if “None” was selected at the Search field. If any other selection was made at the previous field, enter text in this field corresponding to the type of search term selected.

Sort by and Order fields

The Sort by and Order fields are used for specifying the manner in which the generated report view will be sorted.

At the **Sort by** field, make a selection from the pull-down menu for one of the available sort options: “Category Count”, “IP Count”, “User Count”, “Site Count”, “Page Count”, “Object Count”, “Time”, “Hit Count”.

At the **Order** field, make a selection from the pull-down menu for the order in which to display the sort option count: “Ascending”, “Descending”.

Break type field

The Break type field is used for indicating the manner in which records will display for the specified format when the report view is emailed or viewed. This field is available in the Export Drill Down Report pop-up box via the Export Report button, and in the Save Custom Report pop-up box via the Save Report button.

Choose from the available report selections at the **Break type** pull-down menu. Based on the current report view displayed, the selections in this menu might include the main report type such as “Categories”, double break report types such as “Category/IPs” or “Category/Sites”, and triple break report types such as “Category/User/IPs” or “Category/Site/Users”.

For Categories and Category Groups reports, the following report types also are available: Pie Chart (Usernames), Pie Chart (IPs), Bar Chart (Usernames), and Bar Chart (IPs).

For All User Group reports, the following report types also are available: User Group Pie Chart, User Group Bar Chart.

Format field

The Format field is used for specifying the manner in which text from the report view will be outputted. This field is available in the Export Drill Down Report pop-up box via the Export Report button, and in the Save Custom Report pop-up box via the Save Report button.

At the **Format** pull-down menu, choose the format for the report: “MS-DOS Text”, “PDF”, “Rich Text Format”, “HTML”, “Comma-Delimited Text”, “Excel (English)”.

Downloaded from www.Manualslib.com manuals search engine

***NOTES**: For pie or bar chart selections, "PDF" displays grayed out since this is the only output format available for these report types. Information on report formats can be found in the 'Methods for exporting a Drill Down Report' sub-section.*

For double-break reports only

The Amount shown and # Records fields are available in the Export Drill Down Report pop-up box via the Export Report button, and in the Save Custom Report popup box via the Save Report button. These fields are deactivated by default.

***NOTE**: These fields also display in Save Custom Report under the label: For single-break reports only.*

Amount shown field

The Amount shown field is used for specifying how the report view will be sorted. By default, "All Data Shown" displays greyed-out and this field becomes activated when a double-break report type is selected at the Break type field.

At the **Amount shown** field, make a selection from the pull-down menu for an available sort option: "All Data Shown", Top Category Count", "Top IP Count", "Top User Count", "Top Site Count", "Top Page Count", "Top Object Count", "Top Time", "Top Hit Count".

 # Records field

The # Records field is used for specifying the number of records that will display for the selected sort option. By default, "N/A" displays greyed-out and this field becomes activated when a Top item Count is selected at the Amount shown field.

In the activated **# Records** field, the number saved in the Default Options window displays by default. This number can be edited to indicate the number of records to be included in the exported report.

***NOTE**: The Default Top Value entry in the Default Options window is accessible via Default Options in the Settings menu. See the Default Options sub-section in Chapter 2: Customizing the Client of the Enterprise Reporter Web Client User Guide for more information about the Default Top Value.*

For pie and bar charts only

The Generate using field is available in the Export Drill Down Report pop-up box via the Export Report button, and in the Save Custom Report pop-up box via the Save Report button. This field is deactivated by default.

Generate using field

The Generate using field is used for specifying how a Categories pie chart or bar chart will be sorted. By default, "N/A" displays greyed-out and this field becomes activated when a pie or bar chart report type is selected from the Break type pull-down menu.

At the activated **Generate using** field, make a selection from the pull-down menu for the sort option to be used: "IP Count", "User Count", "Site Count", "Page Count", "Object Count", "Time", "Hit Count".

Downloaded from www.Manualslib.com manuals search engine

Methods for exporting a Drill Down Report

A drill down report view can be emailed or viewed in a specified output format via the Export Drill Down Report option.

Email option

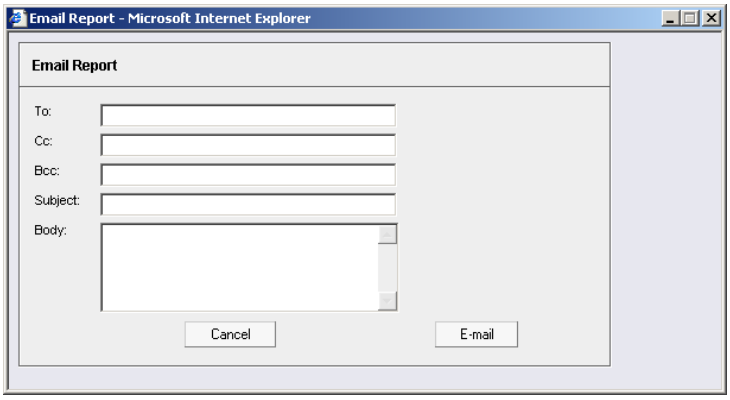
The email option for exporting reports lets you electronically send the report in the specified file format to designated personnel.

***NOTES**: If you are using Lotus Notes as your primary e-mail client instead of Microsoft Outlook or Outlook Express, refer to Appendix B of the Enterprise Reporter Web Client User Guide for information on how to configure Lotus Notes to work with the ER Client.*

For reports generated in the HTML format, the contents of the file will be embedded in the email message. For reports generated in any other format [MS-DOS Text, PDF, Rich Text Format, Comma-Delimited Text, Excel (English)], the file will be sent as an email attachment.

***WARNING**: If using a spam filter on your mail server, email messages or attachments sent by the Client might not be delivered if these messages contain keywords that are set up to be blocked. Consult with the administrator of the mail server for work around solutions between the spam filter and mail server.*

1. In the Export Drill Down Report pop-up box, click the **Email** button to open the Email Report pop-up box:



Email Report pop-up box

2. In the **To** field, enter the email address of each intended report recipient, separating each address by a comma (,) and a space.
3. An entry in each of the following fields is optional:
   - **Subject** - Type in a brief description about the report.
   - **Cc** - Enter the email address of each intended recipient of a carbon copy of this message, separating each address by a comma (,) and a space.
   - **Bcc** - Enter the email address of each intended recipient of a blind carbon copy of this message, separating each address by a comma (,) and a space.
   - **Body** - Type in text pertaining to the report.

***TIP**: Click Cancel to close the Email Report pop-up box and to return to the report view.*

Downloaded from www.Manualslib.com manuals search engine

4. Click **E-mail** to send the report to the designated recipient(s). As a result of this action, the Email Report pop-up box now displays information to indicate the report is being generated.

***WARNING**: Large reports might not be sent due to email size restrictions on your mail server. The maximum size of an email message is often two or three MB. Please consult your mail server administrator for more information about email size restrictions.*

After the report is generated in the specified file format, the Email Result pop-up box displays this message: "The report has been sent to the following address(es)", and lists the email address(es) below:

Email Result - Microsoft Internet Explorer
The report has been sent to the following address(es):
jthomas@logo.com
tjohnson@logo.com

Email Result pop-up box

5. Click the "X" in the upper right corner of the Email Result pop-up box to close it.

View and print options

The view and print options for exporting reports let you view/print the report in the specified file format. The view option lets you make any necessary adjustments to your report file settings prior to printing the report. To print the report, you must have a printer configured for your workstation.

Click the **View** button to begin generating the report in the specified file format. As a result of this action, a window opens displaying the following message: "Please wait for your report to be generated."

After the report is generated in the specified file format, the finished report displays in the browser window.

***NOTE**: Reports generated in the format for MS-DOS Text, Comma-Delimited Text, or Excel (Chinese or English) will display a single row of text for each record. Reports generated in all other formats (PDF, Rich Text Format, HTML) will display any lengthy string of text wrapped around within a fixed column width for each record.*

Downloaded from www.Manualslib.com manuals search engine

View and print tools

In the browser window containing the report, the tools available via the toolbar let you perform some of the following actions on the open report file:

File:

- **Save** (Ctrl+S) or **Save As** - save the report file to your local drive
- **Print** (Ctrl+P) - open the Print dialog box where specifications can be made before printing the report file, such as changing the orientation of the printed page by selecting **Portrait** (vertical) or **Landscape** (horizontal).

Edit:

- **Select All** - highlight the entire text (Ctrl+A), and then Copy (Ctrl+C) and Paste (Ctrl+V) this text in an open file
- Perform a search for text > **Find** - search for specific text in the file (Ctrl+F)

To close the report file window, click the "X" in the upper right corner of the window.

Sample report file formats

The following report file formats are available for emailing and viewing: “MS-DOS Text”, “PDF”, “Rich Text Format”, “HTML”, “Comma-Delimited Text”, “Excel (English)”.

***NOTES**: 8e6 recommends using the PDF and HTML file formats over other file format selections—in particular for detail reports—since these files display and print in a format that is easiest to read. Lengthy text in PDF, HTML, and Rich Text Format files wraps around within the column so all text is captured without displaying truncated.*

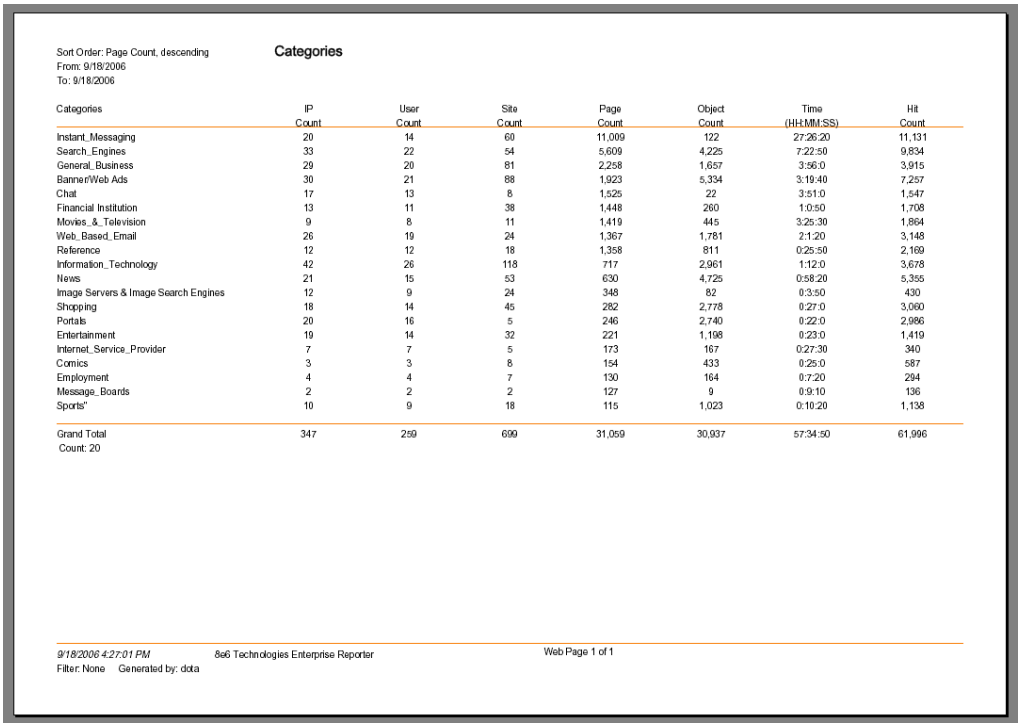
Comma-Delimited Text and Excel report columns may display with truncated text, but an entire column can be viewed by mani-pulating the column width in the generated report file. These reports can then be printed at a smaller percentage than normal size in order to accommodate all text.

For MS-DOS Text reports, text may display truncated—in parti-cular for lengthy usernames and URLs in detail reports—but an entire column can be viewed by scrolling to the right. Since there is no way to manipulate text in the generated report file, the printed report may display with truncated text. However, the maximum amount of text can be captured by printing the report in the landscape format.

Downloaded from www.Manualslib.com manuals search engine

PDF

This is a sample of the Categories report in the PDF format, saved with a .pdf file extension:



Sort Order: Page Count, descending
From: 9/18/2006
To: 9/18/2006

Categories

Categories	IP Count	User Count	Site Count	Page Count	Object Count	Time (HH:MM:SS)	Hit Count
Instant_Messaging	20	14	60	11,009	122	27:26:20	11,131
Search_Engines	33	22	54	5,609	4,225	7:22:50	9,834
General_Business	29	20	81	2,258	1,657	3:56:0	3,915
Banner/Web Ads	30	21	88	1,923	5,334	3:19:40	7,257
Chat	17	13	8	1,525	22	3:51:0	1,547
Financial Institution	13	11	38	1,448	260	1:0:50	1,708
Movies_&_Television	9	8	11	1,419	445	3:25:30	1,864
Web_Based_Email	26	19	24	1,367	1,781	2:1:20	3,148
Reference	12	12	18	1,358	811	0:25:50	2,169
Information_Technology	42	26	118	717	2,961	1:12:0	3,678
News	21	15	53	630	4,725	0:58:20	5,355
Image Servers & Image Search Engines	12	9	24	348	82	0:3:50	430
Shopping	18	14	45	282	2,778	0:27:0	3,060
Portals	20	16	5	246	2,740	0:22:0	2,986
Entertainment	19	14	32	221	1,198	0:23:0	1,419
Internet_Service_Provider	7	7	5	173	167	0:27:30	340
Comics	3	3	8	154	433	0:25:0	587
Employment	4	4	7	130	164	0:7:20	294
Message_Boards	2	2	2	127	9	0:9:10	136
Sports"	10	9	18	115	1,023	0:10:20	1,138
Grand Total Count: 20	347	259	699	31,059	30,937	57:34:50	61,996

9/18/2006 4:27:01 PM 8e6 Technologies Enterprise Reporter Web Page 1 of 1
Filter: None Generated by: dota

Categories report, PDF format

Examples of other report formats are provided in the **Enterprise Reporter Web Client User Guide**.

Downloaded from www.Manualslib.com manuals search engine